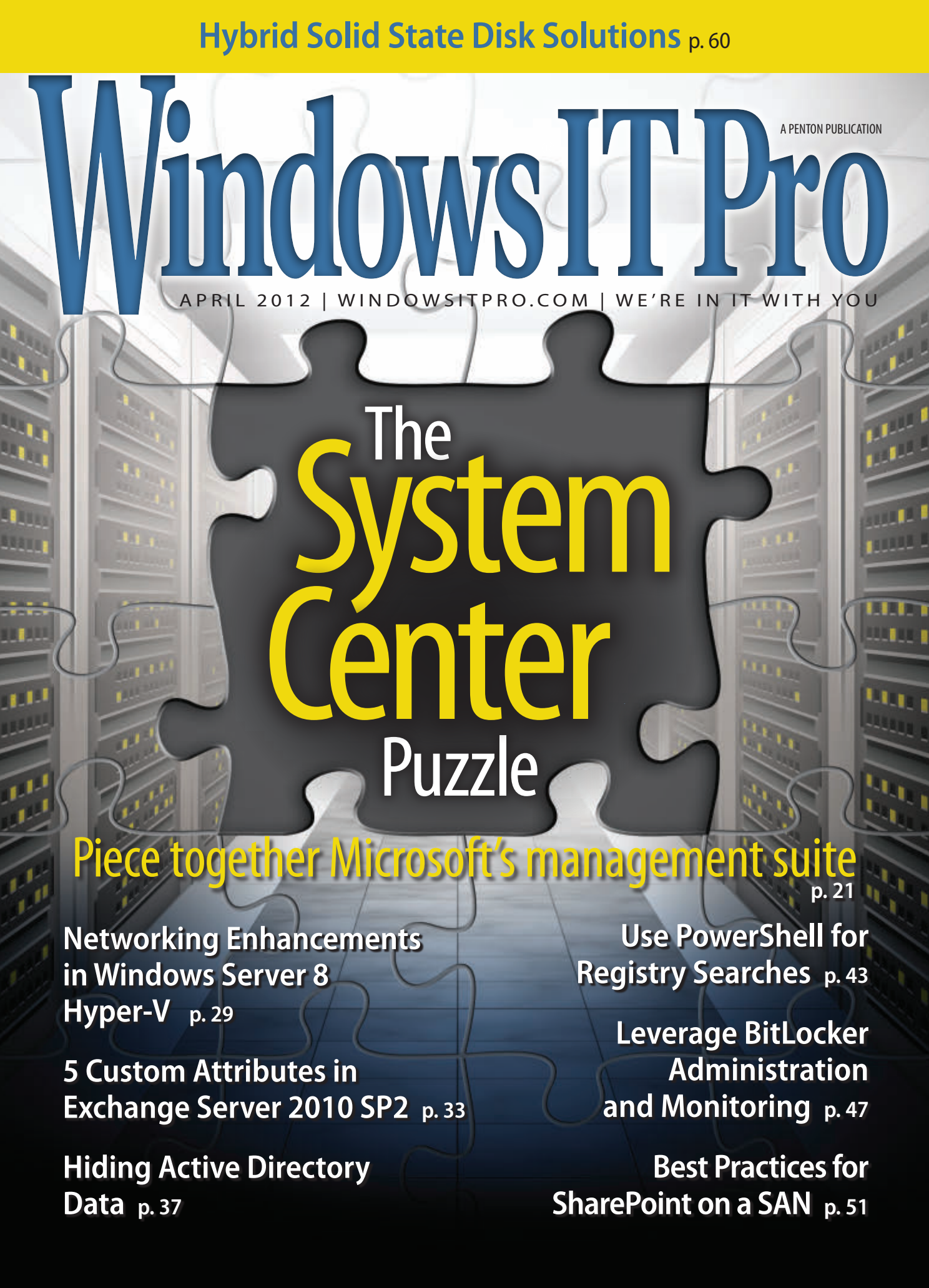
Hybrid Solid State Disk Solutions p. 60

Windows IT Pro

A PENTON PUBLICATION

APRIL 2012 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU



The System Center Puzzle

Piece together Microsoft's management suite p. 21

C O N T E N T S

COVER STORY

FEATURES

INTERACT

IN EVERY ISSUE

Access articles online at www.windowsitpro.com. Enter the article ID (located at the end of each article) in the InstantDoc ID text box on the home page.

Windows IT Pro

A PENTON PUBLICATION

APRIL 2012

VOLUME_18 NO_4

COLUMNS

CONTENTS

PRODUCTS

Windows IT Pro

EDITORIAL

Editorial Director
Megan Keller megan.keller@penton.com

Editor in Chief
Amy Eisenberg amy@windowsitpro.com

Senior Technical Director
Michael Otey motey@windowsitpro.com

Technical Director
Sean Deuby sean@windowsitpro.com

Senior Technical Analyst
Paul Thurrott paul@windowsitpro.com

Industry News Analyst
Jeff James jjames@windowsitpro.com

Custom Group Editorial Director
Dave Bernard dbernard@windowsitpro.com

Exchange & Outlook
Brian Winstead bwinstead@windowsitpro.com

Systems Management, Networking, Hardware
Jason Bovberg jbovberg@windowsitpro.com

Security, Virtualization
Jeff James jjames@windowsitpro.com

SharePoint
Caroline Marwitz cmarwitz@windowsitpro.com

SQL Server, Developer Content
Megan Keller mkeller@windowsitpro.com

Managing Editor
Lavon Peters lavon.peters@penton.com

Editorial SEO Specialist
Jayleen Heft jayleen.heft@penton.com

Editorial Assistant
Blair Greenwood blair.greenwood@penton.com

CONTRIBUTORS

SharePoint and Office Community Editor
Dan Holme danh@intelliem.com

Senior Contributing Editors
David Chernicoff david@windowsitpro.com
Mark Minasi mark@minasi.com
Paul Robichaux paul@robichaux.net
Mark Russinovich mark@sysinternals.com
John Savill john@savilltech.com

Contributing Editors
Alex K. Angelopoulos aka@mvps.org
Michael Dragone mike@mikerochip.com
Jeff Fellinge jeff@blackstatic.com
Brett Hill brett@iisanswers.com
Darren Mar-Elia dmarelia@windowsitpro.com
Tony Redmond 12knocksinna@gmail.com
Eric B. Rux ericbrux@whshelp.com
Curt Spanburgh cspanburgh@scg.net
Bill Stewart bstewart@iname.com
Orin Thomas orin@windowsitpro.com
Douglas Toombs help@toombs.us
Ethan Wilansky ewilansky@windowsitpro.com

ART & PRODUCTION

Production Director
Linda Kirchgesler linda@windowsitpro.com

Senior Graphic Designer
Matt Wiebe matt.wiebe@penton.com

ADVERTISING SALES

Publisher
Peg Miller pmiller@windowsitpro.com

Key Account Director
Chrissy Ferraro christina.ferraro@penton.com 970-203-2883

Manager of IT and Dev Strategy and Partner Alliance
Marie Evans marie.evans@penton.com 970-203-2761

Account Executives
Barbara Ritter barbara.ritter@penton.com 858-367-8058
Cass Schulz cassandra.schulz@penton.com 858-357-7649

Client Project Managers
Michelle Andrews 970-613-4964
Kim Eck 970-203-2953

Ad Production Supervisor
Glenda Vaught glenda.vaught@penton.com

MARKETING & CIRCULATION

Customer Service service@windowsitpro.com

Senior Director, Marketing & Analytics
Tricia Syed tricia.syed@penton.com

Online Sales Development Director
Amanda Phillips amanda.phillips@penton.com 970-203-2761

CORPORATE

PENTON

Chief Executive Officer
David Kieselstein david.kieselstein@penton.com

Chief Financial Officer/Executive Vice President
Nicola Allais nicola.allais@penton.com

TECHNOLOGY GROUP

Senior Vice President, Technology Media Group
Kim Paulsen kpaulsen@windowsitpro.com

WRITING FOR *WINDOWS IT PRO*
Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

LIST RENTALS
Contact MeritDirect, 333 Westchester Avenue, White Plains, NY or www.meritdirect.com/penton.

REPRINTS
Wright's Media
penton@wrightsmedia.com 877-652-5295

GREAT WEB HOSTING
THE BEST VALUE
SERIOUS BUSINESS

Superior Website Availability with 1&1 Dual Hosting for Windows
Your website is simultaneously hosted in 2 locations in our geo-redundant data centers!

Free Domain
with Private Domain Registration.

1&1 BUSINESS WINDOWS PACKAGE

- **UNLIMITED** Web Space
- **UNLIMITED** Traffic
- **UNLIMITED** E-mail Accounts
- Microsoft® SQL Database
- **UNLIMITED 24/7** Support
- Dedicated SSL Certificate

NOW 6 MONTHS FREE!

Then $9.99/month*

YOUR PRIVACY IS IMPORTANT. WE AGREE.

That's why at 1&1, all domains come with FREE Private Domain Registration to protect your name, address, phone number and e-mail from spammers and identity thieves.

MEMBER OF united internet

1-877-461-2631 www.1and1.com
1-855-221-2631 www.1and1.ca

1&1®

* 6 months free offer valid with 12 month minimum contract term only. Upfront payment due upon sign up. Setup fee and other terms and conditions may apply. Private domain registration is available for .com, .net, .org, .info, .biz, .tv, .mobi, .name, .ws, and .cc domains. Visit www.1and1.com for full promotional offer details. Program and pricing specifications and availability subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet, all other trademarks are the property of their respective owners.

James

"Every systems administrator will find this baker's dozen–sized list of free security tools, utilities, and resources useful."

13 Free Security Tools and Resources

Systems administrators will likely find something to add to their toolbox

As I was heading off to the annual security extravaganza known as the RSA Conference in late February, I felt it would be appropriate to highlight some of the best free security tools and services that my fellow editors and external security experts have found invaluable to help them do their jobs. The result is this baker's dozen–sized list of free security tools, utilities, and resources that every systems administrator may find useful.

A big Twitter hat tip goes out to @The_Ajan, @jjx, @xcoppin, @MrsYisWhy, and @ironfog for offering up their security resource suggestions and favorites.

1. Data Breach Investigations Report, Verizon RISK Team

Some of the best security resources aren't tools or software, but quality information and analysis. The annual Data Breach Investigations Report (DBIR)—compiled by the Verizon RISK Team, with help from the U.S. Secret Service and the Dutch High Tech Crime Unit—provides an expansive overview of data breaches and other security incidents.

It's fascinating reading and provides an inside look at the how, the why, and the when of data breaches. You can view the report at http://bit.ly/VerizonRISKReport.

2. ESET SysInspector

Getting a glimpse at all of the processes, startup sequences, network connections, system details, and registry data of a Windows PC can be a difficult task without the right tools. That's when a system utility like ESET's SysInspector (go.eset.com/us/download/free-antivirus-utilities) can come in handy. SysInspector features a slick user interface, a color-coded approach to highlighting potential vulnerabilities, and an active community of users that can help you get the most out of using it.

3. Ettercap

One of the more popular utilities for analyzing network protocols, Ettercap (ettercap.sourceforge.net), is a tool that lets you analyze computers on a network and determine what information they're sending to each other. Like many security tools (and the Force), Ettercap can be used both for good (finding security vulnerabilities) or for evil (executing "man in the middle" attacks).

4. Fyodor's List

There are dozens of security tools and resources available to IT pros and security practitioners, and one of the best places for getting a good summary of all of them is Gordon Lyon's Fyodor's List (sectools.org). This expansive online resource provides information on 125 networking utilities, making it an invaluable ally in helping you find the right software tool for your specific security needs and requirements.

5. KeePass

Keeping track of the plethora of online passwords we all use to access everything from baking information to our Facebook accounts can be a time-consuming chore at best and a severe security vulnerability at worst. Aside from following a sound password selection strategy, having a utility like KeePass (keepass.info) automatically mind your online passwords for you can be a handy solution to your password problems.

6. Microsoft Security Essentials

Years ago, many PC antivirus programs were resource-hogging parasites that seemed to slow a system to a crawl while they were trying to protect it. One of the antivirus programs leading the charge for lighter, faster, and more efficient system protection is Microsoft Security Essentials (windows.microsoft.com/en-US/windows/products/security-essentials), a free, lightweight program that is ideal for personal use or for businesses with 10 or fewer PCs.

7. Network Mapper (Nmap)

One of the more popular open-source applications for network exploration is the accurately (and concisely) named Network Mapper, or Nmap (nmap.org). It also does a fantastic job as a more

Windows IT Pro is going digital!

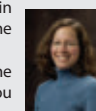
We're excited to announce that starting in May we'll be offering an upgraded digital edition. Although we will no longer offer *Windows IT Pro* in print, the new digital editions will provide the same great content enhanced with audio and video, social media feeds, and other interactive features.

We look forward to continuing to provide in-depth technical content that you can now view on your PC, tablet, or smartphone device. You'll be able to read the digital edition online or offline, and you'll have the ability to print articles on demand.

We have created a landing page with additional information about the transition to digital here: http://www.windowsitpro.com/announcements/subscriber.

Please take a look at the new digital edition when it launches in May and give me your feedback. We are eager to make the magazine as useful as ever.

In the coming months we'll be rolling out tablet and smartphone apps, so let us know what features we can provide that will help you do your job more effectively. Thanks for reading and being part of the *Windows IT Pro* community!



—Amy Eisenberg, Editor in Chief

general network analysis tool, helping you get information on all the services, hosts, OSs, firewalls, and other details of an analyzed network. It's also available for Mac, Linux, and most other major OSs.

8. National Vulnerability Database (NVD)

Good information is sometimes the best tool of all, and the information contained in the National Vulnerability Database, or NVD (www.us-cert.gov/nvd.html), can be a great resource to help you narrow your focus to the most important threats, or help you avoid purchasing or deploying a vendor application that is rife with security holes and vulnerabilities.

9. Qualys BrowserCheck

Having an insecure, out-of-date, or critically vulnerable web browser or browser plug-in can be a big security risk. That's why the free BrowserCheck web service (browsercheck.qualys.com) from Qualys is such a great resource. Simply head to the BrowserCheck website and let it do an analysis of your current browser and affiliated plug-ins. Qualys also offers a business edition that allows admins to get a comprehensive view of all the browsers, plug-ins, and associated vulnerabilities on a specific network.

10. Secunia Personal Software Inspector (PSI)

Most PCs are stuffed with dozens of programs and applications, and keeping all of those potential security vulnerabilities patched and updated can seem like an impossible task. That's where Secunia PSI (secunia.com/vulnerability_scanning/personal) comes in: It does a thorough search of your system, then alerts you to any programs that have available patches and need to be updated. There's also an online version of the app that offers somewhat reduced functionality but lets you sample what the product can do without a download.

11. Splunk

The Splunk marketing team uses the slogan "Finding your faults, just like Mom" to advertise Splunk (www.splunk.com), and it's an apt description. Splunk helps you comb through the mountains of computer-generated information that a modern IT infrastructure produces and helps you examine what's happening, where, and by which files. It's a valuable tool for any security professional's toolbox.

12. TrueCrypt

Keeping vital data secure on the motley menagerie of storage devices that many IT organizations have to support can be an arduous task under the best circumstances. Free open-source disk encryption software like TrueCrypt (www.truecrypt.org) can help: It supports on-the-fly encryption, can be used to encrypt an entire volume (or partition), and can even create mountable virtual encrypted disks within files.

TrueCrypt helps make it far more difficult for unwanted eavesdroppers to snoop on those highly confidential documents about the revolutionary new product your company might be developing (or what you are buying your daughter for her birthday).

13. Wireshark

Wireshark (www.wireshark.org) is a network protocol analyzer that you can use to examine and analyze all of the traffic flowing through a computer network. It's available for many different platforms, supports hundreds of networking protocols and file formats, and has been in continuous development since 1998.

Add to the Discussion

Do you have any favorite security tools you can't live without? Share the wealth by adding a comment to this column at www.windowsitpro.com (InstantDoc ID 142392) or by contributing to a discussion about free security tools on Twitter: @jeffjames3.

InstantDoc ID 142392

JEFF JAMES (jjames@windowsitpro.com) is industry news analyst for *Windows IT Pro*. He was previously editor in chief of Microsoft *TechNet* magazine, was an editorial director at the LEGO Company, and has more than 15 years of experience as a technology writer and journalist.

Among other things, SQL Server 2012 promises improved availability and increased business insight.

But are these features and promised benefits really worthwhile for your organization—and is there anything you should really be excited about?

To find out, join independent SQL Server experts Stacia Misner and Michael K. Campbell for a frank and informative overview of essential SQL Server 2012 features that will provide your organization with practical benefits.

Stacia Misner

Michael K. Campbell

http://elearning.left-brain.com/event/practical-sql-server-2012

Thurrott

"Windows Phone 8 will share key components and user experiences with Windows 8, although some will be tailored for the smaller form factor."

Windows Phone in 2012: Why "Tango" and "Apollo" Will Be Key to Microsoft's Smartphone Success

This year, we can expect two revisions to Windows Phone, one minor and one major. But unlike with previous versions, these releases won't necessarily supersede each other and will instead coexist in the market as we head into 2013. Both are quite important to the future of Windows Phone, despite their minor and major tags, respectively. Has Microsoft finally found a recipe for success in the smartphone market?

Windows Phone "Tango"

The first of these releases, code-named "Tango" and expected by mid 2012, is aimed at broadening the Windows Phone user base. It will do so by undercutting the requirements of the current Windows Phone platform to support lower-end devices that can be sold more cheaply. Microsoft is thought to be working closely with its special partner, Nokia, on this Windows Phone version.

The biggest change to Tango, which will likely be called Windows Phone 7.5.1 when released, is that it will lower the platform's memory requirements. This will usher in a new generation of Windows Phone handsets that utilize just 256MB of RAM.

But it's not just that these handsets will include less RAM, according to my sources. The underlying OS is also being optimized for the lower RAM allotment, with apps certified for this release being required to use less RAM and other resources and certain resource-intensive background tasks being disabled. Developers will be able to target Tango or Windows Phone 7.5 going forward, or both, and users of the new low-end systems will basically be able to access a subset of the existing Windows Phone Marketplace apps selection. (That said, I'm also told that Tango users will be able to browse, but not download, incompatible apps. That's a rather unfortunate prospect.)

This situation will lead to charges that Windows Phone, like Android, is being fragmented. Although true, it's currently unclear how much of the existing Windows Phone apps library will be incompatible with the new devices. I'm told that some high-end games such as "Plants vs. Zombies" won't work, for example, while others such as "Angry Birds" will run normally.

It's clear that Microsoft is pursuing a two-pronged approach that gives it both quantity (Tango) and quality (Windows Phone 8), albeit in two separate product lines that are familial only in that the available apps are (largely) compatible between the two. Given Windows Phone's relatively low impact in the market so far, this strategy is, at least, excusable.

Developers should have received a new version of the Windows Phone SDK by the time you read this, I'm told. This SDK will let developers test apps on both 256MB Tango devices and mainstream 512MB handsets in emulation. Developers can choose to opt out of Tango going forward if they'd like, though that might not be desirable if these devices sell as well as expected.

I've seen rumors that developers will get support for C++ in the Tango SDK, in addition to support for managed code languages such as C# and Visual Basic, but I've not been able to corroborate that. (And I doubt such support would be tied to a minor OS upgrade such as this.) More credible are rumors that Tango will support up to 120 different languages, up from 35 in today's Windows Phone versions. I've not verified that either, but it at least makes sense, given the target markets.

Windows Phone 8 "Apollo" Revealed

Thanks to a leak by the mobility blog Pocketnow, I can now discuss a far more compelling Windows Phone release that will be launched alongside Windows 8. Dubbed Windows Phone 8 and code-named "Apollo," this release is a major one.

Windows Phone 8 is part of the Windows 8 family of products, and it will share core technologies with its desktop- and tablet-based stablemates—including the kernel, multicore processor support, networking stack, security, and multimedia, according to Windows Phone honcho Joe Belfiore. It will also share various user experiences such as the Metro-style UI.

In a leaked video, Belfiore explained that there were two major new functional areas to Windows Phone 8—*Scale and Choice* and *Windows Reimagined*—and four supporting functional areas: *Seamless Communications*, *Lights Up the World Around You*, *Smarter Way to App*, and *Built for Business*. So maybe it makes sense to frame this discussion around those areas.

Scale and Choice. Windows Phone 8 will add support for higher-end processors, including those with dual cores, Belfiore notes in the leaked video. It will also enable up to four different screen resolutions, though he doesn't specify what those are; today's Windows Phone devices support just one, 480 × 800. It will also officially support removable micro-SD expansion for the first time. (And yes, I know that a handful of first-gen Windows Phone devices included this expansion, but Microsoft didn't support it.)

A new feature called Data Sense will help users get the most out of their cellular data plans, while underlying changes to the platform will ensure that Windows Phone 8 uses less data than before.

The system will use Wi-Fi rather than cellular data whenever possible, and a new Kindle Fire–like browser proxy service will make web browsing and third-party app usage 30 percent more efficient. Data Smart will include a dedicated app for managing data usage and a live tile with live data usage stats. The Local Scout feature in Bing is being updated to help find nearby Wi-Fi hotspots, and in many regions, cellular data will be automatically offloaded, when possible, to operator-run Wi-Fi hotspots.

Windows Reimagined. Windows Phone 8 is officially part of the Windows 8 family of systems, and it appears that Windows Phone 8 will fill the gap for devices with smaller screens. Belfiore said that the Metro UI used in both Windows 8 and Windows Phone 8 would become "the new familiar" and that hundreds of millions of people will get Windows 8 on their PCs, laptops, tablets, and, yes, phones, in the year after the whole platform launches. (My sources tell me to expect a Q4 2012 launch for both Windows 8 and Windows Phone 8.)

Windows Phone 8 will share key components and user experiences with Windows 8, although some experiences will be tailored for the smaller form factor, including Internet Explorer 10, which will ship in a special IE 10 Mobile version just on Windows Phone. For developers, hardware makers, and device driver writers, the two platforms are so close that those who "are writing apps or device driver writers can reuse, by far, most of their code, making it easy to target both the phone and the PC," according to Belfiore. The grand unification begins.

Windows Phone 8 and Windows 8 will also share several online services, including SkyDrive and Xbox LIVE. SkyDrive will be used for syncing settings and files between Windows 8–based PCs, devices, and phones, as well as media and other content. Belfiore specifically mentions storing music and Microsoft Office documents on SkyDrive and then accessing that content "magically" from the phone. He notes that the Windows Phone 8 music experience will be able to stream user-uploaded songs from SkyDrive seamlessly.

Microsoft is also killing off the Zune PC client, which is currently required to sync phone-based photos to the PC and to deliver large software updates to the phone. In Windows 8, this app will be replaced by a dedicated companion app for Windows Phone 8. Presumably, those actions that do require Zune software today—phone camera downloads and software updates—will likely be done through the cloud.

Seamless Communications. Windows Phone 8 handsets and Windows 8 devices (primarily tablets, but also some laptops) will also include Near Field Communications (NFC) chips and, as important, exterior "tap points" so that users with these devices can share information. NFC is also used for making secure digital purchases, so Windows Phone 8 will include an integrated Wallet experience, similar, I imagine, to Google Wallet.

Windows Phone 8 will also support an emerging IP Multimedia Subsystem/Rich Communications Suite (IMS/RCS) VoIP standard called RCSe. As with Skype, it will be provided as a dedicated app but also with some integration into the relevant platform pieces, such as the People hub contacts management system. I'm told, however, that Skype will be optional in Windows Phone 8, which I take to mean that certain wireless carriers could leave this feature out of their phones.

> Windows Phone 8 will fill the gap for devices with smaller screens.

Lights Up the World Around You. This nebulous category revolves around the location-aware features of Windows Phone, a fairly obvious area of functionality for any mobile system. This includes various improvements to Bing and Local Scout, but Belfiore didn't offer much explanation. I'm told that Local Scout is picking up personal recommendation capabilities.

Smarter Way to App. Windows Phone 8 will enable a new app-to-app communication capability that appears to be based on Windows 8 Contracts. It will also add native app creation abilities for all developers, and not just for those who partner with Microsoft, as is the case today. This will help developers more easily port games and apps between Windows 8 and Windows Phone 8 and also with iOS and Android, Belfiore claims.

The camera app is being overhauled in Windows Phone 8 to let third-party developers (and Nokia) enhance camera capabilities and even take over the built-in camera app, which Belfiore described as "basic." These so-called "lens apps" offer "mind-blowing possibilities," according to Belfiore.

Microsoft projects that the Windows Phone Marketplace will have over 100,000 "Mango" (Windows Phone 7.5) apps by the time Windows Phone 8 launches. And all of these will be compatible with Windows Phone 8, which is fantastic. Improvements to the Marketplace experience will surface relevant apps during searches more naturally, Belfiore said, and will utilize Bing technologies to deliver real-time results to users.

Built for Business. One of the most exciting aspects of this system is that Microsoft is addressing the business market. Windows Phone 8 will "greatly satisfy IT admins" with full support for Exchange ActiveSync (EAS) policies, including full-disk encryption with BitLocker and the Windows 8 Secure Boot feature. BitLocker will be enabled by default on Windows Phone 8 handsets, Belfiore says, so they're secure by default.

Windows Phone 8 will include updated versions of the Office Mobile apps that are tied to the "Office 15" wave of solutions. It will also include enhanced device management and inventory support through System Center.

Poised for Success

While I might quibble with the two-pronged approach that Microsoft is taking with Windows Phone Tango and Windows Phone 8, there's little doubt that the Windows Phone 8 wave, in particular, will be a huge hit with consumers and businesses alike. It's a renaissance for a product line that deserves more than the scant attention it's received thus far. With Windows Phone 8, Microsoft's mobile OS is finally poised for success.

InstantDoc ID 142238

PAUL THURROTT (paul@windowsitpro.com) is senior technical analyst for *Windows IT Pro*. He writes the SuperSite for Windows (winsupersite.com), a weekly editorial for Windows IT Pro UPDATE (www.windowsitpro.com/email), and a daily Windows news and information newsletter called WinInfo Daily UPDATE (www.wininformant.com).

Business moves faster every day. Keeping up gets tougher. And standing still is falling behind. To get ahead, you need to wring every ounce of productivity out of every department. But it's about more than optimizing technology. It's about optimizing people with the right tools to do more. That's why over 90% of Fortune 1000 companies adopt Condusiv™ Technologies high-performance products. So, how will you keep up with the ever-accelerating pace of business? **For more on how Condusiv can help you Think Faster, visit Condusiv.com or call 888.644.1257.**

Diskeeper is now

Condusiv Technologies

V-locity® | Diskeeper® | Undelete® | ExpressCache®

Minasi

"Although the range of things that you can query *search-adaccount* for is small, those queries are some of the most popular."

A Tale of Two Cmdlets

Piggyback two AD PowerShell cmdlets to achieve maximum efficiency

In my past few columns, I've been talking about the Active Directory (AD) tool called *search-adaccount*. This is a command that you'll appreciate more and more as you continue to explore it. Need to find locked-out users in a particular OU? Easy. Want to know who hasn't logged on in 110 days? Piece of cake. Want to find all of the disabled users in a given OU and retrieve their managers' names so that you can report the accounts to their bosses via email? No prob—oh.

OK, I take that back. That *is* a problem. Apparently, *search-adaccount* can find those users, but it can't tell you their manager's name . . . or those users' titles . . . or those users' given names . . . or just about any of the 100-plus attributes that every AD user object contains. The problem is solvable, but let me back up and explain a bit more.

Thus far, you've met two of Windows Server 8 R2's AD-serving PowerShell cmdlets: Get-ADUser and *search-adaccount*. Get-ADUser, the beefier of the two cmdlets, lets you describe in great detail what sort of users you're trying to extract from AD. That's great, but it carries the cost of fairly complex syntax. The AD folks apparently knew that, however, and must have feared that Get-ADUser would scare would-be AD PowerShellers, so they built a "junior partner" cmdlet for Get-ADUser called *search-adaccount*. *Search-adaccount* can perform only a small percentage of the queries that Get-ADUser can, but its syntax is far less scary than Get-ADUser's. If that sounds like it might be a bad tradeoff, trust me, it isn't: Although the range of things that you can query *search-adaccount* for is small, those queries are some of the most popular. *Search-adaccount* can find accounts with expired passwords, locked-out accounts, disabled accounts, inactive accounts, expired and about-to-expire accounts, and accounts with passwords that never expire. Add that to *search-adaccount*'s much smaller list of parameters, and you end up with a cmdlet that's quite a bit easier for AD PowerShell types to figure out than Get-ADUser. (But let's be clear: I'm not suggesting you give Get-ADUser a pass, as that would be a big mistake. Any AD admin will need it regularly.)

You've also seen that after Get-ADUser does its job, it returns just 17 of the 110 attributes and properties associated with an AD user account, but you can fix that by adding the *-properties* parameter (or *-pr*) to the Get-ADUser statement, as in

```
get-aduser -f "title -like 'teach*'" -properties
  office,title
```

That query would return the 17 standard properties of users, as well as the *office* and *title* properties. Remember also that you can get a list of the particular properties that Get-ADUser provides by piping its output into the cmdlet *get-member* (or *gm*), as in

```
get-aduser -f "title -like 'teach*'" -properties
  office,title | gm
```

Now try piping *search-adaccount*'s output to *get-member* to see what *search-adaccount* offers in the way of properties. Use this query, which should work on any AD implementation because, by default, every AD environment has a disabled account named *guest* and another named *krbtgt:*

```
search-adaccount-accountdisabled -usersonly|gm
```

A quick look at *get-member*'s output will show that it's even stingier with information than Get-ADUser's defaults, with just 13 properties revealed. So how would you, for example, extract the title or office of an account retrieved by *search-adaccount*? My first thought was that *search-adaccount* must have a *-properties* parameter like Get-ADUser's, but unfortunately that's not the case. How, then, to get *search-adaccount* to cough up all the details of an account? Enlist the aid of Get-ADUser! For example, to see all your disabled user accounts and to see their titles and offices, type

```
search-adaccount-usersonly -accountdisabled | Get-ADUser
  -pr title,office
```

The first part of that code finds all the user accounts that are disabled. Then, the pipe (|) says to put those user accounts into the pipeline, feeding them as inputs to the command that follows. The final portion tells Get-ADUser to go get those user accounts from AD, and when it displays the accounts, it should show not only the basic 17 attributes but also the *office* and *title* attributes. It's a nice workaround for a cmdlet limitation, but for the sake of completeness I should mention that the Get-ADUser command ends up being a trifle redundant, as it re-queries AD for those disabled accounts. But the number of disabled accounts will probably be fairly tiny compared with the total number of accounts, so it's not a terrible redundancy. Oh, and in case you've been wondering, you can send email messages from PowerShell, using the *send-mailmessage* command. But I'll cover that another day.

InstantDoc ID 142155

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 30 books.

Otey

"You can call these netsh commands from within your PowerShell scripts."

Windows Firewall Netsh Commands

Configure Windows Server networking and firewall functions from the command line

Today, Windows PowerShell works with just a subset of the Windows Server management functions, although Windows Server 8 will add around 2,300 new Windows PowerShell commands. For now, to configure Windows Server networking and firewall functions, you need to use netsh commands. In this column, I'll show you 10 handy netsh commands you can use to query and configure your Windows Firewall settings. It's worth noting that you can call these netsh commands from within your PowerShell scripts.

10 **Query firewall rules**—You'll probably need to discover Windows Firewall's current configuration properties. You can query Windows Firewall settings with this netsh command:

```
netsh advfirewall firewall show rule name=all
```

9 **Enable and disable Windows Firewall**—Sometimes when you're performing testing or setting up new applications, you need to turn Windows Firewall off for a period. The following commands show how to turn it off and then back on:

```
netsh advfirewall set allprofiles state on
netsh advfirewall set allprofiles state off
```

8 **Reset Windows Firewall**—If you make a mistake configuring Windows Firewall, you can use the following netsh command to reset it back to its default settings:

```
netsh advfirewall reset
```

7 **Set logging**—The default path for the Windows Firewall log files is \Windows\system32\LogFiles\Firewall\pfirewall.log. This command changes the location to C:\temp:

```
netsh advfirewall set currentprofile
  logging filename "C:\temp\pfirewall.log"
```

6 **Control pings**—You can use netsh to control how a given system responds to ping requests. These commands show how to block and then open the firewall to ping requests:

```
netsh advfirewall firewall add rule name="All ICMP V4"
  dir=in action=block protocol=icmpv4
netsh advfirewall firewall add rule name="All ICMP V4"
  dir=in action=allow protocol=icmpv4
```

5 **Enable a port**—One common thing you need to do with Windows Firewall is open ports that are used by programs. The following example shows how to use netsh to create a rule to open port 1433, which is used by Microsoft SQL Server:

```
netsh advfirewall firewall
  add rule name="Open SQL Server Port 1433"
  dir=in action=allow protocol=TCP localport=1433
```

4 **Enable a program**—Another common task is opening Windows Firewall for a given program. The following example illustrates how to add a rule that enables Windows Live Messenger to work through Windows Firewall:

```
netsh advfirewall firewall
  add rule name="Allow Messenger" dir=in action=allow
  program="C:\programfiles\messenger\msnmsgr.exe"
```

3 **Enable remote management**—Another task is to enable remote management so that tools such as Microsoft Management Console can connect to remote systems. To open the firewall for remote management, use this command:

```
netsh advfirewall firewall set rule group=
  "remote administration" new enable=yes
```

2 **Enable Remote Desktop Connection**—For easy remote systems management, use the following command to open Windows Firewall for Remote Desktop Connection:

```
netsh advfirewall firewall set rule group=
  "remote desktop" new enable=Yes
```

1 **Export/import firewall settings**—It's a good idea to export your settings so that you can reapply them later or import them into another system. These commands show how to export and then import your Windows Firewall configuration:

```
netsh advfirewall export "C:\temp\WFconfiguration.wfw"
netsh advfirewall import "C:\temp\WFconfiguration.wfw"
```

InstantDoc ID 142324

MICHAEL OTEY (motey@windowsitpro.com) is senior technical director for *Windows IT Pro* and *SQL Server Pro* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

Deuby

"How do you take a wide range of identity-related data sources and make the consolidated data available to whatever applications need it?"

The Rise of Virtual Directory Servers

Virtualization can simplify your Identity and Access Management environment

Most Identity and Access Management (IAM) systems contain a lot of pieces, and though Active Directory (AD) is usually one of those pieces, it isn't the only one. Virtual directory servers have been around for years, but they're experiencing a dramatic increase in popularity thanks to their strengths and the new requirements of cloud computing. What exactly is a virtual directory server? How is it different from AD or a metadirectory server? Why would you want to use one?

Before I talk about virtual directory servers as a solution, let's outline the problem. Not long ago, identity data came solely from within IT. The best-known example is of course AD, which serves as both a network OS and an identity store. The core AD instance is almost always owned by enterprise IT, and its contents are populated by other IT-owned systems such as HR databases.

And who were the consumers of this identity data? IT-owned enterprise applications that typically had some degree of AD integration. They were members of an AD domain, and they used AD security groups to control access to various parts of the application.

All this was great—if you were an application in an AD forest with all your users, or in a forest with trusts set up to give you access to another forest's users. But what about an application in a forest that would never trust the corporate forest, perhaps due to its location (e.g., in a demilitarized zone—DMZ—or entirely outside the corporate firewall)? What if you weren't a Windows application at all? The challenge for companies is how to take a wide range of identity-related data sources and make the consolidated data available to whatever applications need it.

The Metadirectory Server

The first solution for these scenarios was the metadirectory server. To understand how a metadirectory server works, you need to figure out the "meta" part. To understand what a meta "anything" is, repeat the "anything" in its definition. For example, file metadata is data about the data (such as the *last modified* date), and a metadirectory is a directory of directories. A metadirectory server such as Microsoft's Identity Lifecycle Management (ILM) collects data from a variety of data sources, via connectors that you configure for each source, into a central repository. (In ILM, this is referred to as a metaverse.) Once you have this consolidated identity data, indexed off a unique attribute like an employee number, you can push some or all of the data associated with an employee to many different repositories and applications simultaneously. These applications therefore all have a consistent core set of identity data (though they might use different sets of attributes), regardless of whether they talk directly to each other or not.

For example, a popular use of metadirectory services is to populate an AD forest in a DMZ (supporting an Internet-facing app) with all the user IDs in a particular OU in the corporate forest. Security requirements dictate that there can't be a forest trust between the corporate AD forest and the outward-facing DMZ forest. So how do you enable company employees that must administer or use the DMZ forest to use the same credentials they use in the internal corporate forest (i.e., single sign-on—SSO)? A metadirectory server solves this problem by pushing the appropriate objects and attributes out to the DMZ forest from its metaverse, so the credentials between corporate and DMZ forest are in sync, as you see in Figure 1.

Metadirectory servers are powerful, but they're expensive to purchase, they're expensive to design and deploy, and they have lots of moving parts to maintain once deployed. Another challenge that metadirectory servers are ill-equipped to deal with is identity sources and destinations that may no longer be within the enterprise (e.g., cloud identity providers); IT can't make changes to the sources to fit the metadirectory nor make administrative or technical changes to the endpoint.

Finally, there might be a question of scalability; a metadirectory server moves a lot of identity data around to its various endpoints—even if the endpoints don't need it immediately. Take, for example, an application that has hundreds of thousands of authorized users in its local identity store, which is populated by a metadirectory server. Suppose the application requires the lastLogon attribute from the corporate AD—an attribute that changes regularly. Even if only five users per day log on to this application, all the identity data for all the app's users must be initially pushed to the app. And because its value is updated regularly, lastLogon for many users

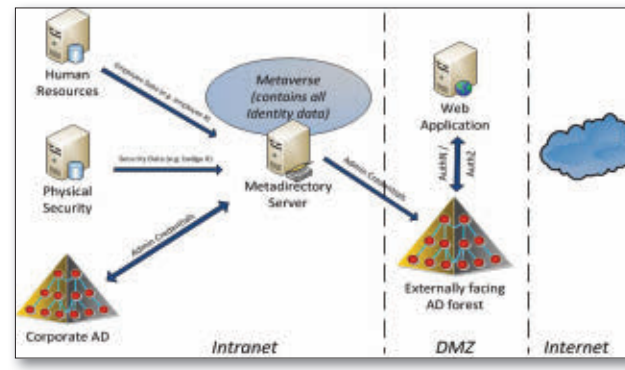


Figure 1: Metadirectory server solution

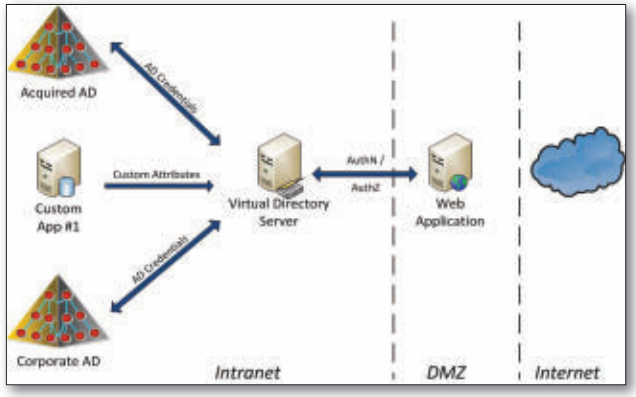


Figure 2: Common virtual directory server scenario

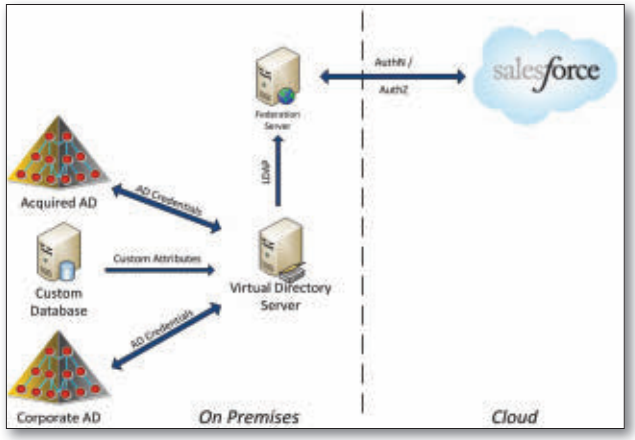


Figure 3: Simplifying your identity federation architecture

must also be pushed to the app at each sync cycle. That's a lot of processing cycles that essentially go to waste.

The Virtual Directory Server

The best way to understand a virtual directory server is to follow a process that's similar to the way I dissected the metadirectory server: Take a good definition of virtualization (I like Edwin Yuen's definition, which says that "virtualization is simply isolating one computer resource from the other resources") and apply it to a directory server. At its simplest, a virtual directory server isolates multiple identity sources at the server's back end to appear as a single, virtual directory for the applications that access the server at its front end.

In contrast to a metadirectory server (which presents a unified view from multiple identity sources by collecting all the source's data into one big metadirectory), a virtual directory server has no equivalent database—it only collects the data required when it's needed. (A cache can be used to improve performance, but nothing on the metaverse scale.) It does this by issuing real-time queries to the appropriate data sources and consolidating the data returned into a single view before presenting it to the server's applications. The apps don't know this identity data view is collected from different data sources; the virtual directory server isolates, or abstracts, the heavy lifting of querying each source for the particular bits of identity data that a given application needs.

Figure 2 shows an example of the most common virtual directory server scenario: simplifying access to a messy identity environment. In this example, an enterprise has a web service that employees can use inside or outside the company. This enterprise has acquired another company; that company's AD forest (still containing its employee accounts) doesn't yet have any trust established with the corporate forest, but the newly acquired company must be able to access the web service. The web service also uses attributes from a custom database. This would be a messy problem to solve with a metadirectory server, involving attribute synchronization with two potentially large forests.

Using a virtual directory server, the solution is pretty straightforward. The virtual directory server is configured to provide the web service with a view that contains the service's needed attributes. The service issues a standard (e.g., LDAP) query to the virtual directory server, which executes a real-time query to its various sources, consolidates the replies into one response, and returns the response to the service, which can use it for authentication or authorization. The virtual directory server provides a layer of abstraction between the web service and its data sources, and the only data that goes over the wire is what's required for a given transaction.

An emerging scenario that plays to virtual directory server technology's strengths is cloud computing and the enterprise. To securely provide access to a cloud service such as Salesforce.com, a federated trust must be established between the identity provider (your enterprise) and the service provider (Salesforce.com). You accomplish this by deploying an on-premises federation server such as Active Directory Federation Services (AD FS) or PingFederate, which performs LDAP queries to your identity environment and constructs tokens to provide to Salesforce.com. You could also use an Identity as a Service (IDaaS) provider, such as Symplified or Okta, to handle the federation for you.

Regardless of how you provide federation, the challenge for many businesses is that their identity environment isn't cohesive. If you plan to use one federation service across the company instead of one per isolated identity store, you must provide one endpoint for the federation service to use. Figure 3 shows how a virtual directory server can work to simplify your identity federation architecture.

Survey Says!

Several years ago, in "Virtual Directories Enhance Identity and Access Management Solutions," Gartner analyst (and former *Windows IT Pro* senior technical editor) John Enck stated, "By year-end 2009, 80 percent of organizations deploying IAM solutions will use virtual directory technology as part of the IAM infrastructure." Has this happened for you? Have you deployed or are you considering a virtual directory server solution? I've created a short survey (www.surveymonkey.com/s/VirtualDirectoryServer) to check up on virtual directory technology's adoption; please take a few seconds of your time to let me know what you're doing!

InstantDoc ID 141861

SEAN DEUBY (sean@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Pro*, and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.

OCT 29 - NOV 1, 2012
BELLAGIO • LAS VEGAS, NV

CLOUD CONNECTIONS

WINDOWS CONNECTIONS

Take the Journey into 2012

Join Microsoft & Industry Experts as New Technologies and Products Release

The industry buzz for Windows 8 and the next release of Microsoft Lync will be hot in fall 2012. You and your team should be in Las Vegas for WinConnections to get the insight and direction your company needs as these products enter the market.

A sampling of speakers CONFERENCE ADVISORY BOARD


JEREMY MOSKOWITZ
MOSKOWITZ, INC.


PAUL THURROTT
WINDOWS IT PRO MAGAZINE


MICHAEL NOEL
CONVERGENT COMPUTING


CHRIS AVIS
MICROSOFT


ASIF REHMANI
SHAREPOINT-VIDEOS.COM


DAN HOLME
AVEPOINT


RANDY WILLIAMS
AVEPOINT


LEE MACKEY
DELL SERVICES


SEAN DEUBY
PENTON MEDIA


DON JONES
CONCENTRATED TECHNOLOGY, LLC


JIM MCBEE
ITNICOS SOLUTIONS


ALAN SUGANO
ADS CONSULTING GROUP


TONY REDMOND
TONY REDMOND AND ASSOCIATES


BRIAN DESMOND
BRIAN DESMOND CONSULTING, LLC


MIKE CROWLEY
PLANET TECHNOLOGIES, INC.

...and many more!

FIND US! facebook.com/winconnections

FOLLOW US! twitter.com/winconnect

Register NOW

This event will sell out. Space is limited.

REGISTER TODAY! www.WinConnections.com • 800.438.6720 • 203.400.6121

Microsoft® Exchange CONNECTIONS

Microsoft® Lync™ CONNECTIONS

UNIFIED COMMUNICATIONS CONNECTIONS

SharePoint CONNECTIONS

SQL Server CONNECTIONS

THE CONVERSATION BEGINS HERE

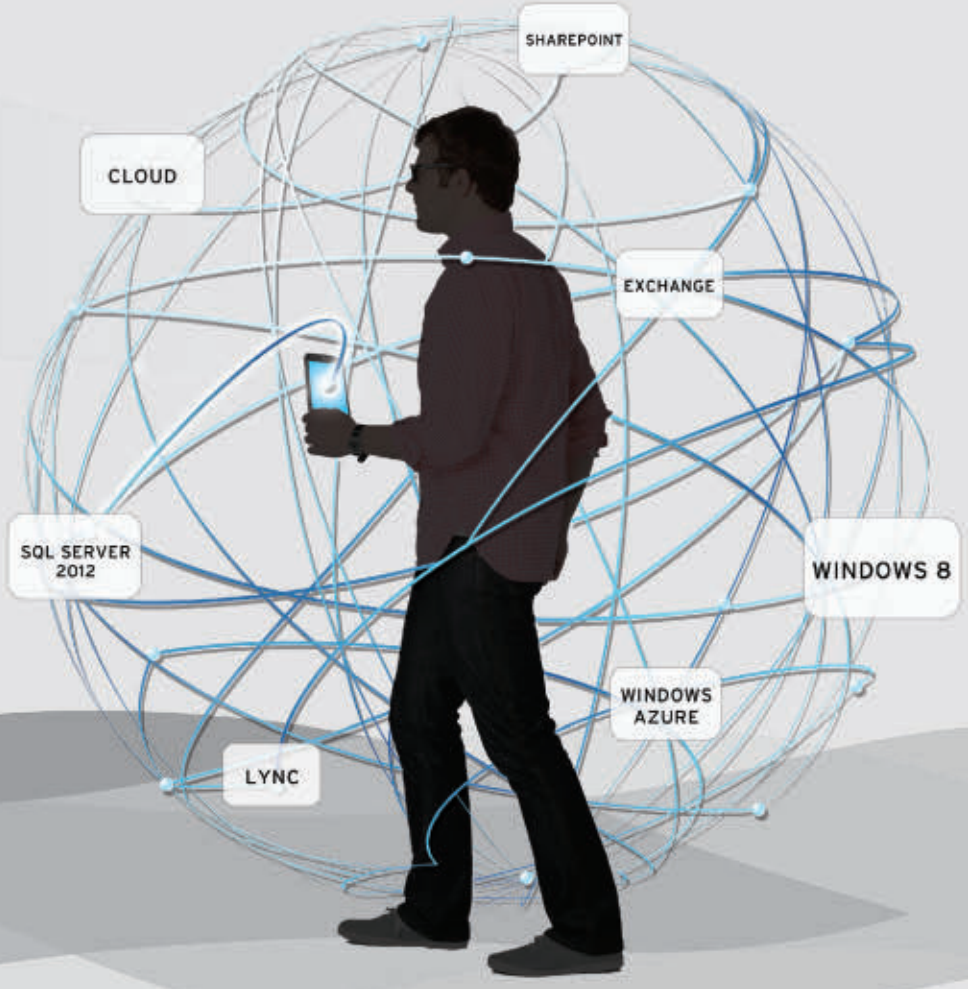
Questions Answered • Strategy Defined • Relationships Built

KEYNOTES

MARK MINASI
MINASI RESEARCH AND DEVELOPMENT

SCOTT GUTHRIE
MICROSOFT CORPORATE VICE PRESIDENT

STEVE FOX
MICROSOFT DIRECTOR



Be Here

- TRAIN WITH 100+ MICROSOFT & INDUSTRY EXPERTS
- OVER 250 IN-DEPTH SESSIONS
- EXCITING NETWORKING PARTIES

REGISTER TODAY! www.WinConnections.com • 800.438.6720 • 203.400.6121

- Hyper-V
- SR-IOV
- Outlook
- System Center 2012
- Windows 8

ANSWERS TO YOUR QUESTIONS

Q: To back up Microsoft SQL Server and Exchange Server servers virtualized with Hyper-V and protected by System Center Data Protection Manager, do I run the DPM agent within the virtual machines or can I just back up at the Hyper-V host level?

A: System Center Data Protection Manager (DPM) offers great backup, continuous protection, and recovery for key Microsoft workloads such as SQL Server, Exchange, SharePoint, file servers, desktops, and Hyper-V. As part of the recovery process, DPM allows item-level recovery from protected workloads, such as restoring a specific SharePoint page or specific SQL Server database instead of the entire server.

DPM also supports backup at the Hyper-V host level. When a backup is performed, the Volume Shadow Copy Service (VSS) request that's issued on the Hyper-V host is actually passed to all the virtual machines (VMs) through the Hyper-V integration services. This ensures the data integrity of the VM backup on the Hyper-V host, because when the VM sees the VSS request it writes all data to disk then pauses writes until the backup is complete.

If a DPM backup is performed at the Hyper-V host level, the only restore option would mean restoring the entire VM or files from the VM, but this wouldn't include items that are application specific, such as a SharePoint document or specific SQL Server database. For application-aware restorations, the DPM protection agent needs to be running within the actual VM that's running the application.

—John Savill

InstantDoc ID 142194

Q: Can I have a single roaming profile on both my 32-bit and 64-bit clients?

A: The sharing of a single profile between 32-bit and 64-bit clients isn't recommended nor is it supported. This is because of the differences in the way both the OS and the applications save settings and data. Ideally you would use a single platform for clients. Or you would use a third-party solution such as AppSense, which separates the user application settings from the normal profile and can handle cross architectures and different OS versions. The Microsoft article "Windows User State Virtualization" (technet.microsoft.com/en-us/library/ff877478.aspx) walks through how to decide upon the right user virtualization solution.

—John Savill

InstantDoc ID 142205

Q: Where are the details on Windows 8 Hardware Certification requirements?

A: Microsoft published Windows 8 requirements for certification in "Windows 8 Hardware Certification Requirements" (msdn.microsoft.com/library/windows/hardware/hh748188). It offers interesting details about the expected hardware specifications for Windows 8 slate devices, in addition to basic OS requirements.

—John Savill

InstantDoc ID 142206

Q: What five virtual machine types does Citrix XenDesktop 5.5 support?

A: Virtual machines (VMs) immediately come to mind when most of us think of XenDesktop 5.5, but this solution actually supports five different VM types, in any combination, to create a Virtual Desktop Infrastructure (VDI).

The Dedicated type is perhaps the most obvious. Dedicated VMs are specifically assigned to individual users, and user state persists between logons. This situation is much different than the Pooled VM type, where a set of VMs is made available to users and user state doesn't persist between logons.

A third VM type, called Existing, is used when XenDesktop is brought in to manage desktops that have been migrated to VMs in the data center. The fourth type, Physical, enables XenDesktop to manage user desktops on dedicated hardware, which can be any physical machine but is most commonly associated with blade PC hardware.

The final, and most flexible, VM type is Streamed. In this scenario, VMs are provisioned to hardware over the network. This type is commonly used in environments that want VDI's benefits without the cost of its accompanying data center–class hardware.

—Greg Shields

InstantDoc ID 142243

Jan De Clercq | jan.declercq@hp.com
William Lefkovics | william@mojavemediagroup.com
John Savill | jsavill@windowsitpro.com
Greg Shields | virtualgreg@concentratedtech.com

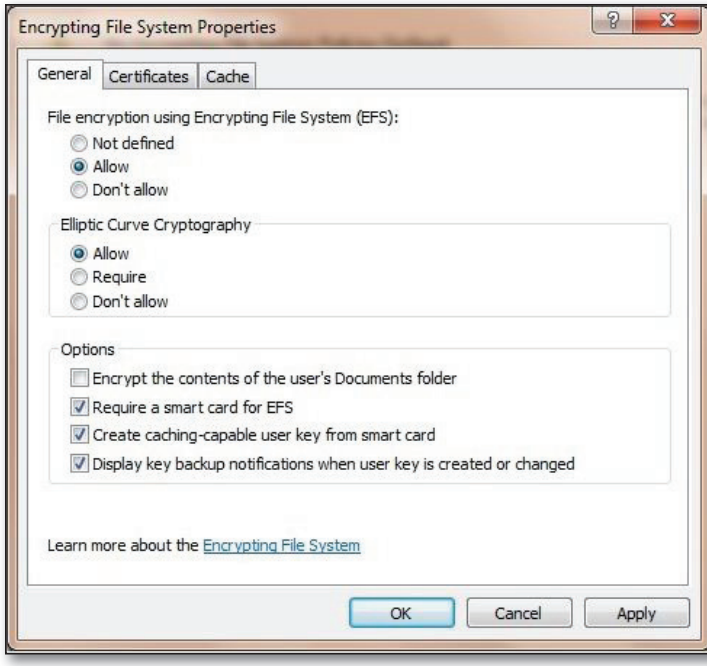


Figure 1: The Encrypting File System Properties dialog box

Q: Can I store my Encrypting File System private key on my smart card?

A: Yes, starting with Windows Server 2008 and Windows Vista, Microsoft supports storage of the Encrypting File System (EFS) private key on a user's smart card. Microsoft provides a Group Policy Object (GPO) setting that will require the use of a smart card for EFS. You can find this setting in the properties of the Encrypting File System container in the \Computer Configuration\Windows Settings\Security Settings\Public Key Policies folder.

As Figure 1 shows, the Encrypting File System Properties dialog box includes the *Create caching-capable user key from smart card* configuration option. This setting lets the administrator select either the cached or non-cached mode of operation for the EFS private key storage on smart cards.

Non-cached mode means that all EFS decryption operations that require the user's private key are done on the smart card. Cached mode means that Windows automatically derives a special symmetric key from the user's private key and caches it in protected system memory on the computer, not on the smart card. Cached mode implies that all standard EFS operations that normally involve the user's private key are replaced with symmetric cryptographic operations that use the special symmetric key.

Cached mode positively affects EFS performance when using smart cards for private key storage. This is because EFS doesn't need to call on the smart card processor for every EFS encryption or decryption operation. Cached mode also eliminates the need to keep the user's smart card plugged in to the smart card reader. You can enable the EFS cached mode of operation for the EFS private key storage on smart cards by selecting the *Create caching-capable user key from smart card* option on the General tab in the EFS properties dialog box, as Figure 1 also shows.

—Jan De Clercq

InstantDoc ID 142075

Q: What is the new licensing model for System Center 2012?

A: Prior to System Center 2012, there were many different products in the System Center family. It made for a fairly long list:

- System Center Configuration Manager
- System Center Operations Manager
- System Center Virtual Machine Manager
- System Center Data Protection Manager
- System Center Service Manager
- Opalis

Each had its own licensing for management licenses. Some had different versions that included SQL Server. Some required that you also pay for the actual management servers. And, of course, you could also purchase the entire suite. In total, there were over 30 different ways to license System Center.

For System Center 2012, the licensing has been simplified. System Center 2012 is now a single product that's comprised of all the System Center components with the addition of System Center App Controller, System Center Endpoint Protection, and Opalis, which has been renamed as System Center Orchestrator. Although in the past each product in the System Center family was a different version, with System Center 2012, each component is now being updated to have a single version number.

The System Center 2012 product comes in two license versions for the servers being managed, and you no longer buy a separate Management Server software license for each component. The list below shows System Center 2012 components (note that you'd also need to add the SQL Server runtime licenses unless the included standard SQL Server rights are used):

- System Center Configuration Manager
- System Center Operations Manager
- System Center Virtual Machine Manager
- System Center Data Protection Manager
- System Center Service Manager
- System Center Orchestrator
- System Center App Controller
- System Center Endpoint Protection

Both licenses have exactly the same components and exactly the same capabilities. Both are licensed in two-processor increments (note that this is per socket, not per core). The difference is in the virtual rights:

- System Center 2012 Standard Edition—offers two OS instances; use this for physical boxes or very lightly virtualized environments.
- System Center 2012 Datacenter Edition—offers unlimited OS instances; use this for virtualized environments.

Clients with existing System Center licenses that are covered by Software

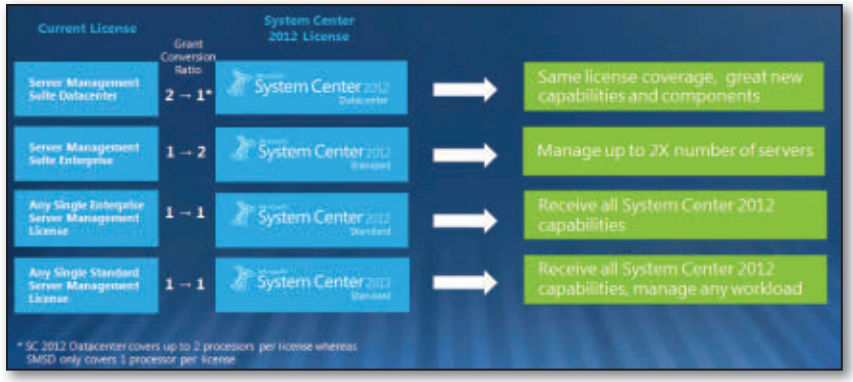


Figure 2: System Center 2012 grant for Software Assurance users

Assurance get a grant for the new System Center 2012 product (see Figure 2). The grant is based on the current license. For more information, see the link for the datasheet PDF at the Microsoft System Center 2012 Release Candidate webpage (www.microsoft.com/en-us/server-cloud/system-center/default.aspx).

—John Savill

InstantDoc ID 142207

Q: What is the new System Center 2012 Unified Installer?

A: System Center 2012 consists of many components that were previously separate products, such as System Center Configuration Manager and System Center Operations Manager. But even though System Center 2012 is now a single product, each component has its own installation processes and requirements. The System Center 2012 Unified Installer enables a simple deployment of all of the System Center 2012 components for testing and proof-of-concept purposes. It does so by deploying each component to its own OS instance (two for System Center 2012 Service Manager) with its own local SQL Server instance, through a single wizard. Using the Unified Installer streamlines installation, reducing the process from 421 installation screens to 16, allowing a complete deployment in around three hours.

The Unified Installer isn't intended for production environment rollouts but is a great way to quickly get the complete System Center 2012 product deployed in a testing environment to start digging into the functionality and learning. The Unified Installer works with physical and virtual OSs. The user provisions the actual OSs first (which must be Windows Server 2008 R2 SP1), joins them to the domain, then passes the OS names to the Unified Installer for the deployment of the System Center 2012 components.

—John Savill

InstantDoc ID 142209

Q: What is SR-IOV?

A: Single Root I/O Virtualization (SR-IOV) is a PCI-SIG standard to provide native I/O virtualization to PCI Express (PCIe) devices. The official specification can be found at the PCI-SIG website (www.pcisig.com/specifications/iov/single_root). Essentially, the technology allows a single PCI Express network device to represent itself as multiple separate devices (all the same type).

An SR-IOV device consists of a Physical Function (PF) object with full PCI Express configurability—essentially the physical NIC object and multiple Virtual Function (VF) objects. These VF objects can't be configured individually but support data movement. They do this through their own individual transmit-and-review queues and lightweight PCIe resources to enable the transmitting and receipt of data, acting like separate network adapters.

These VFs can be attached to a virtual machine (VM), giving the VM direct access to the network device. The number of VFs supported by network adapters varies by device: For example, the Intel 82576 device (1Gbps) supports eight VFs per physical port, while the 82599 device (10Gbps) supports 64 VFs per port.

Although the maximum theoretical number of VFs per port is 256, because the network device needs the resources to support the VF, such as queues for data, data address space, command processing, and more, the actual number implemented in most cards is much lower than 256.

The benefit of using SR-IOV over standard network virtualization is that the VM is talking directly to the network adapter by using Direct Memory Access (DMA). It isn't going through any virtualization transports such as the VMBus nor is processing performed in the management partition since the network packet isn't going through any virtual switch.

Because of this direct communication, the best performance is attained, and it's close to bare-metal performance. It's important to understand that with SR-IOV, the VM is talking directly to the network adapter. This might mean the VM loses some portability since it's no longer abstracted from the physical hardware (the VM will load a VF driver), unless the hypervisor has some capability to handle moving VMs between SR-IOV and non SR-IOV capable hardware. To use SR-IOV, the network card, the motherboard, and the hypervisor all have to support SR-IOV for the VFs to function and be available to the VMs.

—John Savill

InstantDoc ID 142151

Q: Does Hyper-V support SR-IOV?

A: Windows Server 2008 R2 Hyper-V doesn't support SR-IOV. However, Windows Server 8 Hyper-V does include SR-IOV support, including the ability to seamlessly move virtual machines (VMs) between hosts with and without SR-IOV capabilities, without any service interruption and using SR-IOV when it's available.

—John Savill

InstantDoc ID 142152

Q: How can you use QR codes with Outlook 2010?

A: Quick Response (QR) codes are a mechanism for encoding information into a two-dimensional space, such as a barcode interpreted on two axes. A wide range of information can be stored in a QR code, including names, addresses, text content, dates, and phone numbers. This

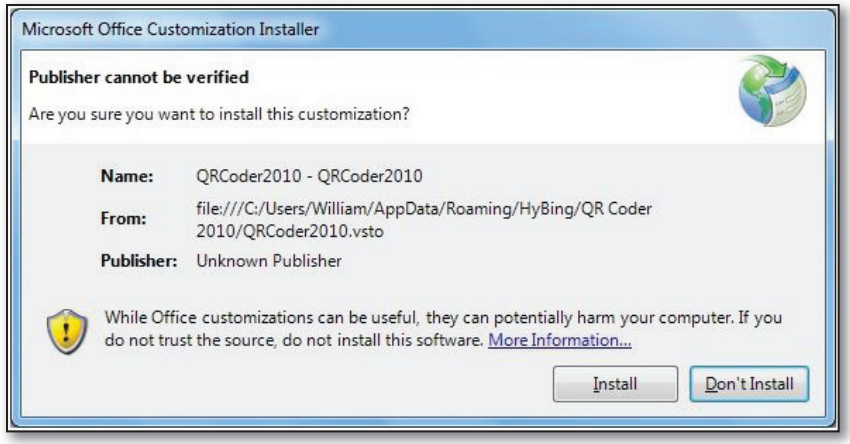


Figure 3: Warning dialog box to install an Outlook add-in from an unknown publisher

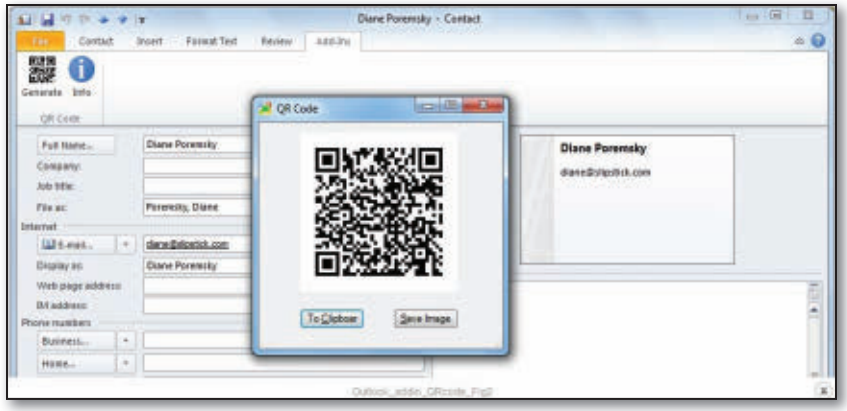


Figure 4: A QR code generated from Outlook by QR Coder 2010

coding form was originally developed for the auto industry in the 1990s; however, its application is universal, especially now that smartphones can interpret these codes. Smartphones and tablets are all equipped with cameras, which can photograph or "scan" QR codes. But what if you want to combine this technology with Microsoft Outlook?

To use QR codes, you need something to encode the data into the square matrix QR code and something to interpret the graphic code on another device. A company called HyBing has developed a QR coder that generates QR codes of Outlook items right from Outlook 2010. HyBing's application, called QR Coder 2010, is free for personal use, with a $2.00 fee for business use (www.hybing.com/QR-Coder-2010.html).

QR Coder 2010 requires the .Net Framework 4.0 or later and Outlook 2010. The installation is as simple as installations can be, as long as you ensure Outlook isn't running at the time. When you open Outlook after installation, you might have to "install" the add-in as an unknown publisher, as Figure 3 shows.

When the add-in is loaded, you access QR Coder through the Add-Ins tab of the Ribbon. With an Outlook item selected, such as a contact, calendar item, or task, the QR Coder Generate button is available in the Add-Ins menu. Figure 4 shows the QR code created when I clicked Generate for a basic contact. This code can then be copied or saved as an image file. The image file can be printed or included in marketing material or perhaps on a business card.

Smartphones with suitable QR readers can then consume the image, interpret the content, and read or save it to their resources. This process eliminates middleware such as email servers for transferring information. In person, information can be transferred directly to the device.

QR readers are available for all flavors of smartphone. I use NeoReader for Windows Phone 7. For a list of QR readers, see 708 Media's website (www.708media.com/qrcode/qr-code-readers-iphone-android-blackberry-windows-phone-7).

—William Lefkovics

InstantDoc ID 141782

Q: What is XDPing used for?

A: XDPing is a command-line tool used to check for common misconfiguration problems in a Citrix XenDesktop environment. You can run it from a XenDesktop console or remotely. It provides information about network interfaces and settings, device DNS lookups and reverse lookups, time synchronization, logged-in users, environment and domain membership, Windows Firewall status and ports, XenDesktop services, and more. It can also check event logs for known events that are related to XenDesktop.

—Greg Shields

InstantDoc ID 142248

Q: Where can I try "Cut the Rope" in Internet Explorer?

A: To showcase the capabilities of Internet Explorer and HTML5, an HTML5 version of the popular "Cut the Rope" game was created. It's freely available at www.cuttherope.ie. It has both a standard and high-definition version and is great to play.

—John Savill

InstantDoc ID 142204

Q: Where does the SMI-S provider for my SAN actually reside?

A: Storage Management Initiative-Specification (SMI-S) is an industry standard that enables a common approach for interacting with storage systems such as SANs. The SMI-S provider runs on a separate OS instance, such as Windows server (which could be virtualized), and provides the SMI-S service to communicate with the SAN. Or it can run on the SAN itself. When the SMI-S client is configured, it needs to point to the SMI-S provider and not the SAN. Thus, if the SMI-S provider isn't hosted on the SAN, you must identify where the SMI-S provider has been installed and point the SMI-S client to it.

—John Savill

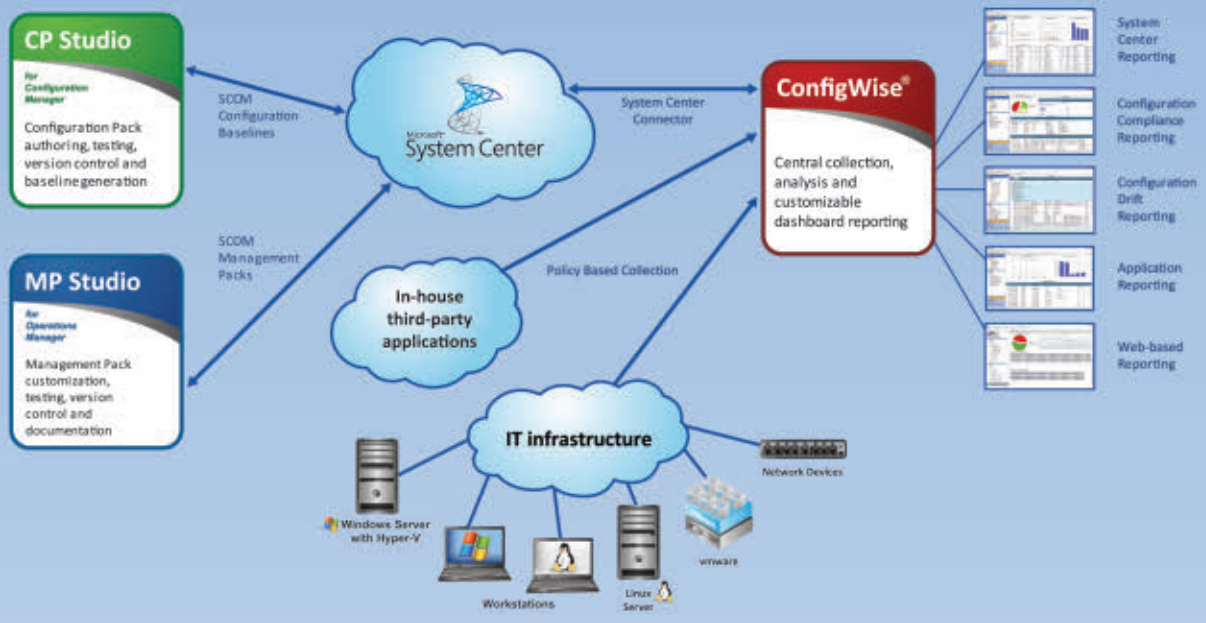
InstantDoc ID 142187

Silect SOFTWARE INC
www.silect.com

NEW ConfigWise for SCCM 2012 reporting edition
*Use promo code "ITPRO" for your free copy***

Get Wise

ConfigWise | MP Studio | CP Studio



Configuration Compliance
Gain enterprise configuration insight and ensure proactive policy compliance by regularly assessing your physical and virtual infrastructure according to regulatory, security or corporate standards with Silect's **ConfigWise**. Leverage industry expertise and best practices with out-of-the-box templates, including baselines from Microsoft Security Compliance Manager and SCAP.

Central Dashboard Reporting
Quickly and easily collect, analyze and report on system and application information across physical and virtual environments with Silect's **ConfigWise**. Create customizable reporting dashboards according to business needs without complex report development or application integration. Deliver business intelligence to report users with web-based report viewing.

System Center Management
Using Microsoft System Center? Improve the deployment and management of Operations Manager and Configuration Manager with Silect's **MP Studio** and **CP Studio** and deliver custom reporting dashboards with information collected from any System Center component, all integrated within a single view with **ConfigWise.**

www.silect.com

***See www.silect.com for details about this free offer – some limitations apply*

Microsoft System Center 2012

Configure and manage apps, services, computers, and VMs

by Orin Thomas

The Microsoft System Center suite recently underwent a major overhaul. All the products in the suite have been revised and are being released as part of Microsoft System Center 2012. System Center is a collection of products designed to help IT professionals configure and manage applications, services, computers, and virtual machines (VMs) in midsized to large enterprises. Each product in the System Center line lets IT pros manage greater numbers of applications, services, computers, and VMs than they would otherwise be able to. Although most people are aware of Microsoft System Center Operations Manager and System Center Configuration Manager, System Center 2012 is composed of a total of eight System Center products:

- Orchestrator
- Virtual Machine Manager
- App Controller
- Operations Manager
- Configuration Manager
- Endpoint Protection (included with Configuration Manager)
- Service Manager
- Data Protection Manager

With the release of System Center 2012, you can install all the components from a single unified installer, as Figure 1 shows. It's also possible to deploy the components in the traditional manner, one product at a time.

System Center 2012 provides several general improvements in all the revised products. These improvements include:

- All products in the System Center 2012 suite are designed with interoperability in mind.
- All products now use a standard UI that was present in more recent versions of System Center products, such as Service Manager, but that wasn't available in older products, such as Configuration Manager.
- Products have similar infrastructure requirements. All versions support the same SQL Server back end, which means that organizations no longer need to support different versions of SQL Server to support their System Center infrastructure. All versions can be installed on Windows

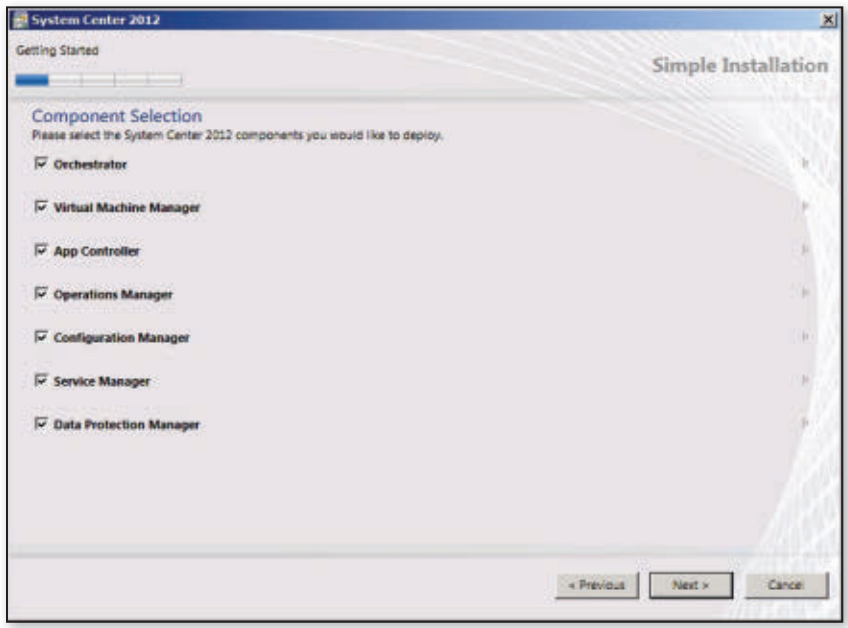


Figure 1: Using Microsoft System Center 2012's Unified Installer

Server 2008 R2 without requiring you to download a substantial number of extra components.

- All System Center products are now designed to be deployed within VMs running on supported hypervisors.
- All System Center products have improved PowerShell support. Newly created PowerShell cmdlets let you accomplish almost all of the tasks available in each product's GUI. Some products include more than 100 new PowerShell cmdlets.
- Improved role-based access control (RBAC) functionality lets you delegate the ability for people to perform specific management and monitoring tasks without giving them unnecessary privileges.

Let's take a look at each of the eight System Center 2012 products. Understanding how each of the components works, what's new in each product, and how each component fits into the System Center suite as a whole can help make your life as an administrator much easier.

Operations Manager

Operations Manager is the System Center monitoring solution. Operations Manager is one of the products in the System Center suite that most IT pros are familiar with, and many administrators have deployed Operations Manager 2007 R2 or its predecessors on the networks they manage.

You can use Operations Manager to monitor the performance and diagnostic output of applications, services, servers, clients, and network devices. You configure Operations Manager to generate alerts to notify you when a particular condition occurs (e.g., a service failing, a disk queue length counter falling outside a specific set of values). Through Microsoft's acquisition of AVIcode and its integration into Operations Manager, you can also use Operations Manager 2012 to carry out performance monitoring and diagnostics of .NET and JEE applications.

Operations Manager 2012 lets you do the following:

- Monitor service, application, server, and network device availability
- Monitor server performance, raising alerts when performance counters exceed or fall below specific thresholds
- Monitor service, application, server, and network device diagnostic information
- Monitor heterogeneous environments with computers running Windows, UNIX, and Linux OSs
- Monitor services and applications across traditional deployments, as well as private and public clouds
- View service and application dependency information across multiple locations, including both public and private clouds

The key to using Operations Manager is adding management packs. Management packs are collections of stored wisdom about specific products so that Operations Manager alerts are generated for things that you, as someone who manages that product, need to know about. For example, the Exchange Server 2010 Monitoring Management Pack for Operations Manager includes the Exchange team's knowledge about the product, including what circumstances warrant raising an alert to get an IT pro's attention.

Operations Manager management packs exist for all major Microsoft products

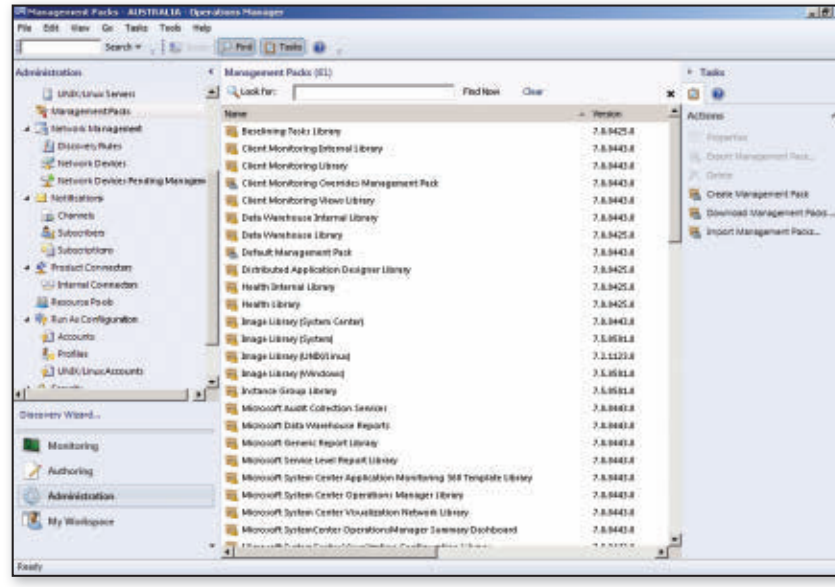


Figure 2: Built-in Operations Manager management packs

(see Figure 2). Many third-party vendors of products that run on Microsoft platforms also publish management packs. For vendors that don't provide management packs to support their products directly, there's also a vibrant third-party management pack authoring industry. If you can't find a management pack for your product, Operations Manager includes tools you can use to create one yourself.

Configuration Manager

Microsoft System Center Configuration Manager (SCCM), formerly Microsoft Systems Management Server (SMS), is another well-known System Center product. System Center 2012's new Configuration Manager lets you manage the deployment and configuration of servers, clients, and devices on your organization's network.

You can leverage Configuration Manager to do the following:

- Deploy customized server and client OSs
- Deploy Microsoft and third-party applications to Configuration Manager clients
- Deploy software updates for Microsoft OSs and applications, as well as deploy updates to third-party applications
- Generate an inventory of all hardware devices installed on Configuration Manager clients
- Generate an inventory of the software configuration of Configuration Manager clients
- Determine how often specific applications deployed to clients are actually being used, through software metering
- Determine if the configuration of Configuration Manager clients meets a particular baseline, including application version, update installation, registry key settings, and the presence of specific files
- Deploy and manage endpoint protection, including anti-malware and firewall configuration, through System Center Endpoint Protection 2012
- Improve mobile device management, including management of devices running iOS and Android

Configuration Manager 2012 includes the ability for organizations to be more user-centric in the deployment of applications. You can configure Configuration Manager so that an application follows a user, no matter which device he or she is using. For example, the application might deploy as a traditional MSI (Windows Installer file) on the user's primary machine, stream through App-V when the user is logged on at another computer, and have a special version delivered to the user's phone. Figure 3 shows the Configuration Manager security roles.

Endpoint Protection

With the release of System Center 2012, Microsoft Forefront Endpoint Protection has been folded into Configuration Manager to let you manage software updates, anti-malware software deployment, and anti-malware and firewall configuration from a single console.

Endpoint Protection anti-malware policies let you configure the following, as Figure 4 shows:

- Scheduled scan type, time, scan-when-idle, force definition update before scan, and limiting scan CPU utilization
- Scan targets, including email and attachments, removable USB drives, network drives, and archived files

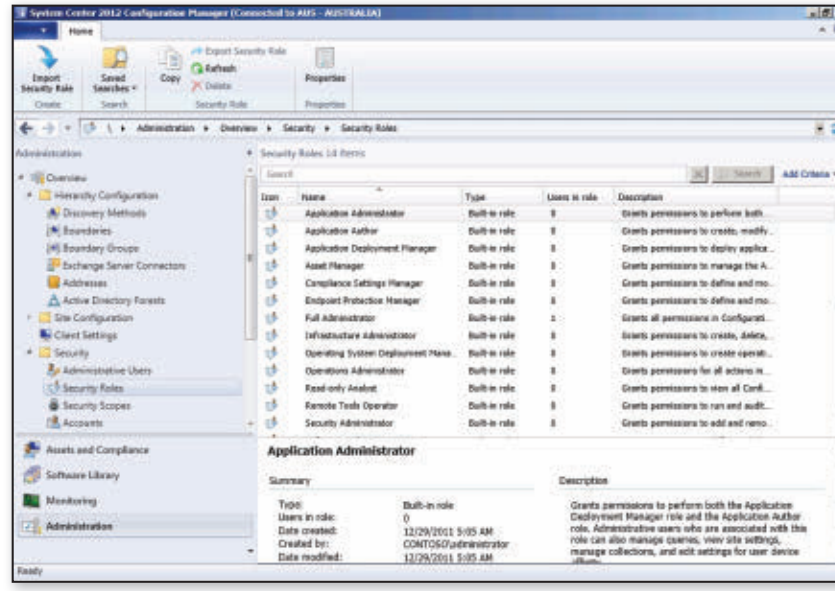


Figure 3: Configuration Manager security roles

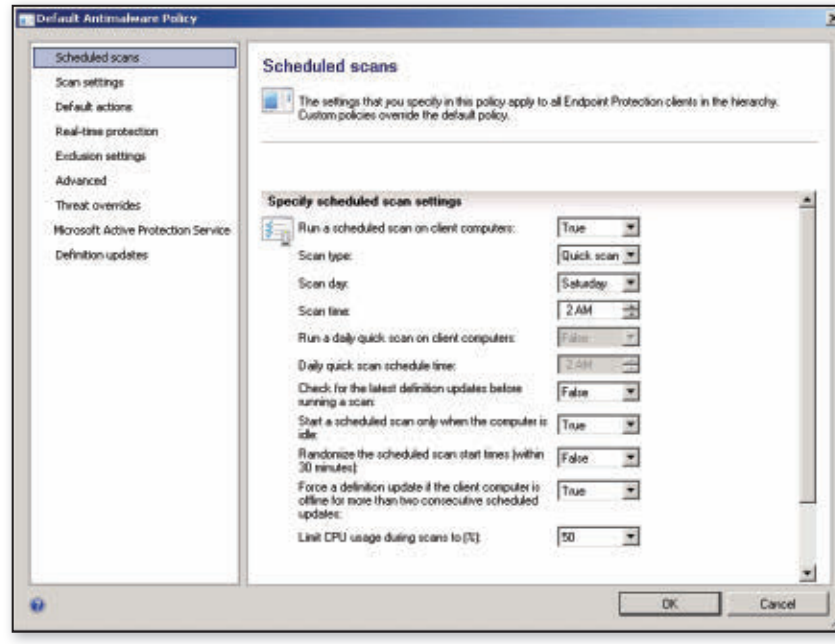


Figure 4: Configuring an anti-malware policy

- Real-time protection, including downloaded files, protection against network exploits, behavior monitoring, and script scanning
- Excluded files, folders, file types, and processes
- Whether restore points are created before disinfecting machines and how long to wait before deleting quarantined files
- Definition update frequency and whether to obtain updates from other sources in the event that the Configuration Manager server can't be contacted

A big benefit of the System Center 2012 release is related to licensing, with Endpoint Protection being included in a Core Client Access License (CAL). Therefore, if you have a license to use Configuration Manager with a client, it includes an Endpoint Protection license.

Data Protection Manager

Data Protection Manager (DPM) is Microsoft's enterprise backup solution. You can use DPM to ensure the reliable backup and recovery of Microsoft workloads, such as Exchange Server, SQL Server, Dynamics CRM, SharePoint, and Windows server and client. You can also back up third-party applications with DPM 2012, as long as there's an appropriate Volume Shadow Copy Services (VSS) writer.

New versions of DPM tend to provide the product with a broader workload, such as DPM 2010's inclusion of remote client backup and Hyper-V item-level recovery. One of the big new features for DPM 2012 is the ability to manage multiple DPM 2012 servers through a single Operations Manager 2012 console. This addresses a limitation in previous versions of DPM in which administrators needed to log on to multiple DPM servers when managing data protection across large environments because each DPM server was limited to protecting 100 production servers, 3,000 clients, and 2,000 SQL Server databases. Beyond what's available in the recently released DPM 2010, DPM 2012 also offers optimized SharePoint item-level recovery, improved reporting, and the ability to be granular with permissions through RBAC. Figure 5 shows the new DPM console.

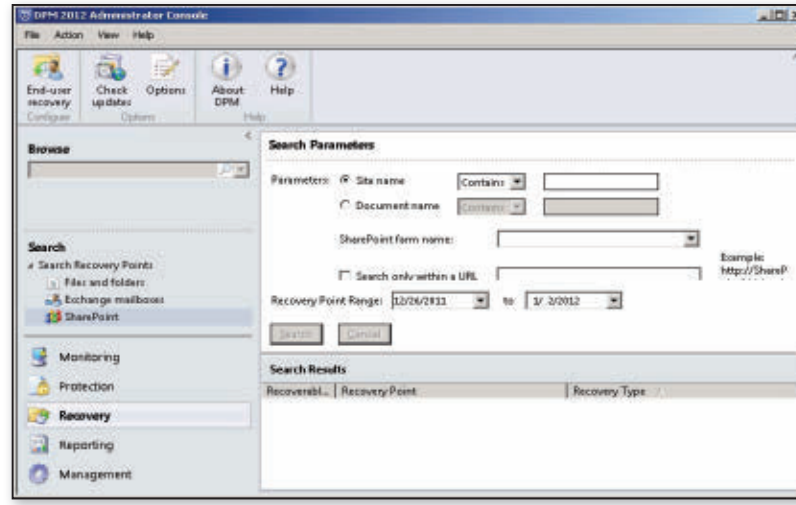


Figure 5: DPM console

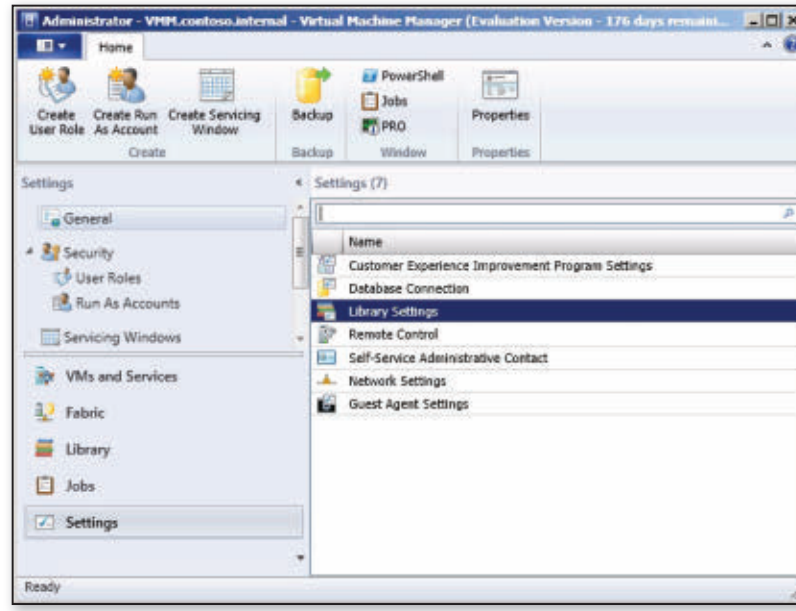


Figure 6: VMM console

Virtual Machine Manager

Virtual Machine Manager (VMM) is Microsoft's enterprise virtualization solution. VMM goes beyond the capabilities available in the Hyper-V console that's built in to Windows Server 2008 R2 and Windows Server 2008 and lets you manage all VMs in the enterprise. VMM 2012 has a functionality focus that reflects Microsoft's Private Cloud strategy. VMM 2012 provides more than just VM management capability. Figure 6 shows the VMM console.

You can use VMM 2012 to accomplish the following goals:

- Manage VMs across multiple hypervisors
- Create and manage clouds, services, host groups, and VMs
- Manage third-party hypervisors, including Xen and VMware
- Perform live physical-to-virtual migrations
- Perform live VM migration from one hypervisor to another
- Rapidly provision VMs based on templates
- Leverage intelligent workload placement based on target hypervisor capacity and performance load
- Manage virtual network and storage pools
- Use the Server Application Virtualization (App-V) feature to simplify deploying server applications by creating a portable server application image

we're not just making servers. we're making server history.

While innovation comes rapidly in the IT industry, basic server architectures haven't changed for decades. That's why Cisco answered the need for innovation by introducing the Cisco Unified Computing System – which integrates compute, high-speed networking, storage access and virtualization in one system. Since its introduction, IT departments have dramatically reduced data center complexity while:

- Lowering operating costs by up to 30%
- Reducing Microsoft deployment times from weeks to minutes
- Harnessing the power of the UCS architecture for Microsoft Window Server and Exchange, SharePoint, and SQL Server deployments

The Cisco Unified Computing System, powered by intelligent Intel® Xeon® processors, signals the next evolution of the data center – where everything, and everyone, works together like never before.

Find out more at www.cisco.com/go/microsoft

together we are the human network. cisco.

Figure 7: App Controller console

- Define multi-tier services that consist of VMs and applications, and then deploy them to the fabric as simply as you would a traditional VM template in earlier versions of VMM

App Controller

App Controller is a new product in the System Center line that lets you configure self-service management of applications hosted on both public and private clouds. App Controller works by letting you delegate role-based views and control of your organization's VMM 2012 private cloud services and Windows Azure services. For example, a user who is delegated the appropriate App Controller role can migrate cloud-based applications between private and public clouds. You can install App Controller only on a computer that has the VMM 2012 console.

App Controller lets you create a library of templates for services that have predefined configuration values. Depending on the role assigned to a user, the user can use the App Controller self-service portal to spin up cloud-based applications based on these templates. App Controller uses a web-based portal rather than a traditional System Center management console. Figure 7 shows the App Controller console.

Service Manager

System Center Service Manager is Microsoft's service desk solution. Service Manager fully integrates with other products in the System Center suite. For example, you can leverage the intelligence stored in products such as Operations Manager and Configuration Manager to automatically populate a service desk job with diagnostic and configuration information as a way to help IT pros resolve tickets.

You can do the following with Service Manager:

- Use it as a standard IT service desk job tracking system; Service Manager lets you track job resolution against differing service level agreements (SLAs) to determine if your service desk is meeting its targets

Service Manager fully integrates with other products in the System Center 2012 suite.

- Leverage SQL Server Reporting Services (SSRS) to generate sophisticated reports on the problems resolved by the IT service desk
- Track specific unit costs for storage, network, and compute resources in private cloud scenarios
- Integrate with Operations Manager to automatically log service desk jobs and notify the appropriate staff when Operations Manager raises an alert
- Automatically resolve some types of service requests without requiring the intervention of an IT pro
- Configure other service request types to be processed after approval is given by appropriate service desk staff
- Integrate with Configuration Manager to allow self-service software deployment; leverage Configuration Manager to view software and hardware inventory of specific users or computers when investigating a service desk request
- Integrate with VMM to allow sophisticated self-service VM deployment
- Utilize new Service Catalog and Release Management features
- Provide third-party access to the Service Manager Data Warehouse

You can build sophisticated workflow processes into Service Manager. For example, you can configure a self-service portal so that users are able to request applications from a certain list that will install automatically and other applications that will install subject to approval. The approval process is handled through Service Manager and can be as sophisticated or as streamlined as necessary.

Orchestrator

Orchestrator, formerly known as Opalis, lets you automate and integrate all of the other System Center products. It isn't a server in the sense that products like Configuration Manager and Operations Manager are but is instead a tool that lets you tie everything together with a specific focus on orchestrating the System Center 2012 suite. Orchestrator uses a drag-and-drop interface for building automation sequences known as *runbooks*. For example, you can use Orchestrator to create a runbook that, triggered by an alert in Operations Manager, uses VMM to deploy a VM from a template, uses Configuration Manager to deploy software to the new VM, configures DPM to automatically protect data sources on the new VM, and then logs all the details as a completed job in Service Manager. Figure 8 shows an Orchestrator runbook.

The benefit of Orchestrator to IT pros is that it allows automation without the complexity of creating elaborate scripts in PowerShell. The drag-and-drop interface makes automating common tasks across the System Center suite simple. It takes very little time for even the most script-o-phobic IT pro to create effective and functional runbooks.

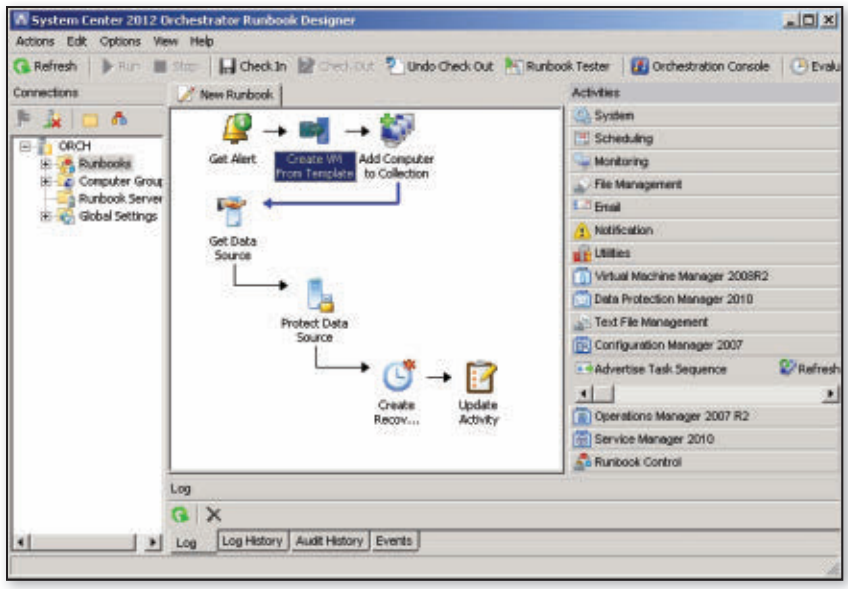


Figure 8: Orchestrator runbook

Orchestrator uses integration packs, which are collections of discrete tasks, such as *Create VM from Template, Add Computer to Collection, Start/Stop Service,* or *Run Program.* Orchestrator also includes tools that let you create your own integration packs. Because Opalis was originally a third-party product before Microsoft acquired it, several third-party vendors such as VMware and IBM Tivoli have created Orchestrator integration packs for products that run on Windows.

You can also call Orchestrator runbooks directly from System Center Service Manager. Therefore, support staff can directly trigger complex jobs from the Service Manager console. More important, end users who have the appropriate privileges can trigger Orchestrator runbooks from self-service portals. For example, a DBA could use a Service Manager self-service portal to trigger a backup snapshot to be taken of a database prior to making changes, without having to contact the DPM administrator to perform the task.

Licensing

Unlike earlier versions of the System Center products, in which each product could be purchased separately, Microsoft plans to sell System Center 2012 as a bundle and not as separate products. System Center 2012 will be available in Standard and Datacenter editions. Both editions include the same eight products. The difference is that the Standard edition supports two OS environments. These environments can be VMs or physical machines, either on premises on in the public cloud. The Datacenter edition supports an unlimited number of on-premises OS environments or eight OS environments in a public cloud environment. Microsoft claims that half of existing customers that deploy System Center products deploy the entire suite, so this approach of including everything is likely to simplify licensing for most organizations.

Licenses are necessary only for the endpoints being managed. For example, the same license will cover managing, backing up, and orchestrating a file server, or a server with SQL Server installed, or Exchange, or Dynamics, and so on.

Although the most efficient way to license large numbers of client computers is through the Core CAL and Enterprise CAL suites, System Center–specific client licensing comes in three flavors:

- Configuration Manager clients can be licensed on a per-user or per-OS environment basis, or in the Core CAL or Enterprise CAL suites.
- Endpoint Protection is available on a per-user or per-device basis, or in the Core CAL or Enterprise CAL suites.
- System Center Client Management Suite is also available on a per-user or per-OS environment basis, as well as in the Enterprise CAL suite. It includes licensing for DPM, Operations Manager, Service Manager, and Orchestrator.

For more information, see the Microsoft System Center 2012 licensing page at www.microsoft.com/licensing/about-licensing/SystemCenter2012.aspx.

Looking Ahead

If leveraged properly, System Center 2012 can fundamentally change the relationship between the IT department and the rest of the organization. Integration between Service Manager, Orchestrator, and other products will let IT departments provide web portals to offer a large number of services automatically that in the past would have required the direct intervention of IT pros. Users can directly request software and services, and the IT department can create workflows in which direct approval can be granted when necessary and automatically when appropriate.

The increased PowerShell support in System Center 2012 and the simplicity with which sophisticated automation can be created through Orchestrator runbooks mean that IT pros can automate a growing number of complex tasks. These changes will allow IT pros to accomplish more with less and will help change the IT strategy from reactive to proactive.

At the Microsoft Management Summit (MMS) 2011 last March, Microsoft announced that the company would continue to release System Center products in a coordinated fashion. Microsoft also stated that releases of System Center products would be more frequent, with the sort of gap between the release of major versions of Operations Manager and Configuration Manager a thing of the past. These assertions suggest that the next revision of all products in the System Center suite will occur sometime in the 2014–2015 timeframe.

InstantDoc ID 141827

Orin Thomas
(orin@windowsitpro.com) is a contributing editor for *Windows IT Pro* and a Windows Security MVP. He has authored more than two dozen books for Microsoft Press and is the convener of the Melbourne System Center User Group.

Paul Thurrott...

. . . he's not in Microsoft's pocket, but now he can be in yours.

The independent voice for IT enthusiasts

Paul Thurrott delivers news, tips, commentaries, and reviews on Microsoft technology – from gaming to mobile to servers to software, and coverage of Microsoft competitors in between. Get daily updates without reaching farther than your pocket.

Download your
Paul Thurrott: PocketTech app today

windowsitpro.com/mobile-apps

Available for iPhone | Windows Phone 7 | Android

Windows Server 8 Hyper-V Networking

Enhancements in the new OS support a variety of cloud scenarios

by John Savill

No man is an island. Nor should your virtual machines (VMs) be, if you want them to do anything useful. Networking is the central nervous system of the data center, allowing communication between all the various parts of your environment. As demands on the infrastructure increase and more companies move to virtualization, the need for site resiliency increases as well. Networking must constantly evolve to meet these increasing demands.

Fortunately, Windows Server introduces a slew of new technologies. These technologies enable Windows Server systems and virtual environments to meet all manner of new requirements and scenarios, including private and public cloud implementations. Often, this type of scenario involves a single infrastructure that's shared by different business units or even different organizations. Server 8 has been optimized for cloud solutions. This will become apparent when I walk through the technologies for networking alone: Nearly all networking areas have been enhanced in some way for Server 8.

In this article, I'll cover three primary areas of Server 8 Hyper-V network features:

- Network virtualization
- Hyper-V virtual switch extensibility
- Enhancements to support new network hardware capabilities and improved Quality of Service (QoS)

Other great capabilities include a new site-to-site VPN solution; huge enhancements to the Server Message Block (SMB) protocol, enabling VMs to run from a Server 8 file share; native NIC teaming; and consistent device naming. But I want to focus on the major network technologies that most affect virtualization.

Network Virtualization

Virtualization has always striven to abstract one resource layer from another, giving improved functionality and portability. But networking hasn't embraced this goal, and VMs are tied to the networking configuration on the host that runs them. Microsoft System Center Virtual Machine Manager (VMM) 2012 tries to link VMs to physical networks through its logical networks feature, which lets you create logical networks such as Development, Production, and Backup. You can then create IP subnets and virtual LANs (VLANs) for each physical location that has a connection to a logical network. This capability lets you create VMs that automatically connect to the Production network, for example; VMM works out the actual Hyper-V switch that should be used and the IP scheme and VLAN tag, based on the actual location to which the VM is deployed.

This feature is great. But it still doesn't solve scenarios in which I might be hosting multiple tenants that require their own IP schemes, or even one tenant that requires VMs to move between different

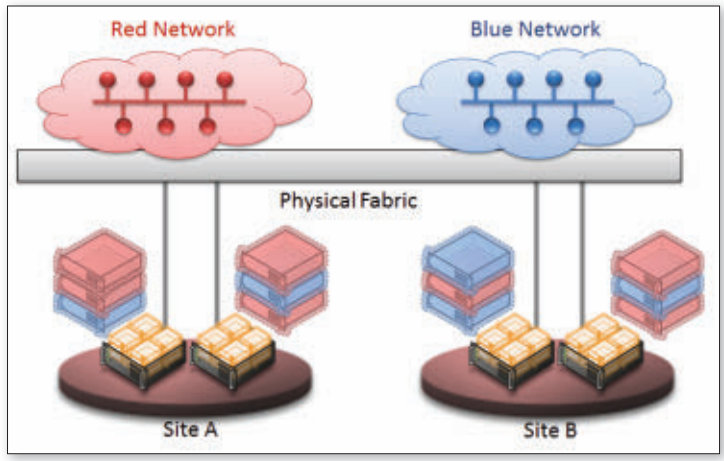


Figure 1: Virtual networking example

locations or between private and public clouds, without changing IP addresses or policies that relate to the network. Typically, public cloud providers require clients to use the hosted IP scheme, which is an issue for flexible migration between on-premises and off-premises hosting.

Both scenarios require the network to be virtualized, and the virtual network must believe that it wholly owns the network fabric, in the same way that a VM believes it owns the hardware on which it runs. VMs don't see other VMs, and virtual networks shouldn't see or care about other virtual networks on the same physical fabric, even when they have overlapping IP schemes. Network isolation is a crucial part of network virtualization, especially when you consider hosted scenarios. If I'm hosting Pepsi and Coca-Cola on the same physical infrastructure, I need to be sure that they can't see each other's virtual networks. They need network isolation.

This virtual network capability is enabled through the use of two IP addresses for each VM and a virtual subnet identifier that indicates the virtual network to which a particular VM belongs. The first IP address is the standard address that's configured within the VM and is referred to as the customer address (using IEEE terms). The second IP address is the one that the VM communicates over the physical network and is known as the provider address.

In the example that Figure 1 shows, we have one physical fabric. Running on that fabric are two separate organizations: red and blue. Each organization has its own IP scheme, which can overlap, and the virtual networks can span multiple physical locations. Each VM that is part of the virtual red or blue network has its own customer address. A separate provider address is used to send the actual IP traffic over the physical fabric.

You can see that the physical fabric has the network and compute resources and that multiple VMs run across the hosts and sites. The color of the VM coordinates with its virtual network (red or blue). Although the VMs are distributed across hosts and locations, the hosts in the virtual networks are completely isolated from the other virtual networks with their own IP schemes.

Two solutions—IP rewrite and Generic Routing Encapsulation (GRE)—enable network virtualization in Server 8. Both allow completely separate virtual networks with their own IP schemes (which can overlap) to run over one shared fabric.

IP rewrite. The first option is IP rewrite, which does exactly what the name suggests. Each VM has two IP addresses: a customer address, which is configured within the VM, and a provider address, which is used for the actual packet transmission over the network. The Hyper-V switch looks at the traffic that the VM is sending out, looks at the virtual subnet ID to identify the correct virtual network, and rewrites the IP address source and target from the customer addresses to the corresponding provider addresses. This approach requires many IP addresses from the provider address pool because every VM needs its own provider address. The good news is that because the IP packet isn't being modified (apart from the address), hardware offloads such as virtual machine queue (VMQ), checksum, and receive-side scaling (RSS) continue to function. IP rewrite adds very little overhead to the network process and gives very high performance.

Figure 2 shows the IP rewrite process, along with the mapping table that the Hyper-V host maintains. The Hyper-V host maintains the mapping of customer-to-provider addresses, each of which is unique for each VM. The source and destination IP addresses of the original packet are changed as the packet is sent via the Hyper-V switch. The arrows in the figure show the flow of IP traffic.

GRE. The second option is GRE, an Internet Engineering Task Force (IETF) standard. GRE wraps the originating packet, which uses the customer addresses, inside a packet that can be routed on the physical network by using the provider address and that includes the actual virtual subnet ID. Because the virtual subnet ID is included in the wrapper packet, VMs don't require their own provider addresses. The receiving host can identify the targeted VM based on the target customer address within the original packet and the virtual subnet ID in the wrapper packet. All the Hyper-V host on the originating VM needs to know is which Hyper-V host is running the target VM and can send the packet over the network.

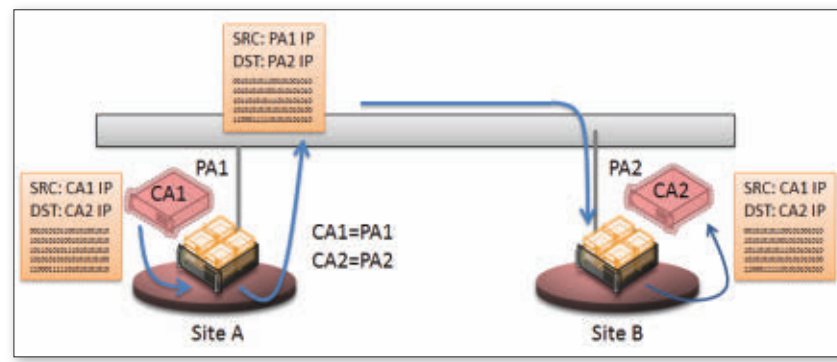


Figure 2: IP rewrite process

The use of a shared provider address means that far fewer IP addresses from the provider IP pools are needed. This is good news for IP management and the network infrastructure. However, there is a downside, at least as of this writing. Because the original packet is wrapped inside the GRE packet, any kind of NIC offloading will break. The offloads won't understand the new packet format. The good news is that many major hardware manufacturers are in the process of adding support for GRE to all their network equipment, enabling offloading even when GRE is used.

In the GRE process, the Hyper-V host still maintains the mapping of customer-to-provider address, but this time the provider address is per Hyper-V host virtual switch. The original packet is unchanged. Rather, the packet is wrapped in the GRE packet as it passes through the Hyper-V switch, which includes the correct source and destination provider addresses in addition to the virtual subnet ID.

In both technologies, virtualization policies are used between all the Hyper-V hosts that participate in a specific virtual network. These policies enable the routing of the customer address across the physical fabric and track the customer-to-provider address mapping. The virtualization policies can also define the virtual networks that are allowed to communicate with other virtual networks. The virtualization policies can be configured by using Windows PowerShell, which is a common direction for Server 8. This makes sense: When you consider massive scale and automation, the current GUI really isn't sufficient. The challenge when using native PowerShell commands is the synchronous orchestration of the virtual-network configuration across all participating Hyper-V hosts.

Both options sound great, but which one should you use? GRE should be the network virtualization technology of choice because it's faster than IP rewrite. The network hardware supports GRE, which is important because otherwise GRE would break offloading, and software would need to perform offloading, which would be very slow. Also, because of the reduced provider address requirements, GRE places fewer burdens on the network infrastructure. However, until the networking equipment supports GRE, you should use IP rewrite, which requires no changes on the network infrastructure equipment.

Extensible Hyper-V Virtual Switch

One frequent request from clients has been the ability to add functionality to the Hyper-V switch—functionality such as enhanced packet-filtering capabilities, firewall and intrusion detection at the switch level, switch forwarding, and utilities to help sniff data on the network. Windows already has rich capabilities around APIs and interfaces, specifically network device interface specification (NDIS) filter drivers and Windows Filtering Platform (WFP) callout drivers, that let third parties integrate with the OS. The Hyper-V extensible switch uses the same interfaces that partners are already using, making it easy for vendors to adapt solutions to integrate directly into the Server 8 Hyper-V extensible switch. There are four specific types of extension for the Hyper-V switch, as Table 1 shows.

Notice that these extensions don't completely replace the Hyper-V switch. Rather, they enhance it, enabling organizations to be specific about the layers of additional functionality that are required within the environment, without needing to perform a complete switch replacement. Because the extensions are embedded within the Hyper-V switch, the capabilities apply to all traffic, including VM-to-VM traffic on the same Hyper-V host and traffic that traverses the physical network fabric. The extensions fully support live migration and can be managed by using GUI tools, Windows Management Instrumentation (WMI) scripting, and PowerShell cmdlets, providing a consistent management feel across the extensions and core Hyper-V capabilities. The extensions for the Hyper-V switch are certifiable under the Windows 8 certification program, helping the extensions to meet an expected level of quality.

Get the Most from Your Hardware

Software enhancements can go only so far. At some point, hardware needs to change to provide new capabilities and performance levels. Thankfully, in recent years there have been many hardware enhancements to networking, mainly in the 10Gb world. Server 8 can leverage 10Gb Ethernet to take advantage of these enhancements.

QoS. When you look at a cloud scenario that functions as both public and private and that can have multiple tenants, meeting service level agreements (SLAs)—including network bandwidth availability—with different tenants becomes extremely important. One VM mustn't consume all the network bandwidth, starving other VMs. In today's converged fabrics, in which network and storage use a shared physical cable, keeping one type of traffic from using more bandwidth and storage than is desired is also vital.

Server 8 includes a Hyper-V QoS capability that uses PowerShell to make it easy to set weights for VMs, in addition to setting minimum bandwidth allocations. These settings help VMs get the required amount of bandwidth in times of contention. When there's no contention, VMs can consume

Table 1: Hyper-V Switch Extension Types

Extension	Purpose	Potential Examples	Extensibility Component
Network Packet Inspection	Inspecting but not altering network packets	Network monitoring	NDIS filter driver
Network Packet Filter	Injecting, modifying, and dropping network packets	Security	NDIS filter driver
Network Forwarding	Third-party forwarding that bypasses default forwarding	Virtual Ethernet Port Aggregator (VEPA) and proprietary network fabrics	NDIS filter driver
Firewall/Intrusion Detection	Filtering and modifying TCP/IP packets, monitoring or authorizing connections, filtering IPsec-protected traffic, and filtering remote procedure calls (RPCs)	Virtual firewall and connection monitoring	WFP callout driver

the available bandwidth to be as high-performing and responsive as possible.

This software QoS is focused at a virtual switch port level. Hardware QoS is also available, by using a new capability in many of today's network infrastructures: Data Center Bridging. DCB allows classification of all the network traffic that's being sent over the physical NIC, whether the traffic is from the Hyper-V host or a VM. In Server 8, the traffic can be divided into eight buckets by using classifications. One bucket could be for iSCSI traffic, another for SMB, and a third for general IP traffic. For each bucket, DCB can configure how much bandwidth is allocated, so that no single type of traffic consumes all bandwidth.

When you consider software QoS and hardware QoS with DCB, the big difference is that software QoS occurs at a VM level and works through the Hyper-V switch, whereas hardware QoS is VM-independent and works across all types of traffic going over the network. Therefore, hardware QoS enables guaranteed service levels for different types of traffic across a single fabric.

Single Root I/O Virtualization. Another great enhancement that takes advantage of NIC improvements is Single Root I/O Virtualization. SR-IOV allows one PCI Express network device to represent itself as multiple devices to VMs. This means that a physical NIC can actually present multiple virtual NICs, which in SR-IOV terms are called virtual functions (VFs). Each VF is of the same type as the physical card and is presented direct to specific VMs. The communication between the VM and the VF now completely bypasses the Hyper-V switch, because the VM uses Direct Memory Access (DMA) to communicate with the VF. Therefore, the communication between the VM and VF is very fast and very low-latency. Neither the VMBus nor the Hyper-V switch is involved in the network flow from the physical NIC to the VM, as Figure 3 shows. Because the Hyper-V switch is bypassed, any features that are exposed through the virtual switch (such as switching, ACL checking, QoS, DHCP Guard, and third-party extensions) no longer apply to the traffic that uses SR-IOV, improving network performance.

With traditional Hyper-V networking, all traffic flows between the physical NIC and the VM through the Hyper-V Layer 2 virtual switch. With SR-IOV, the virtual switch is completely bypassed, as Figure 3 shows.

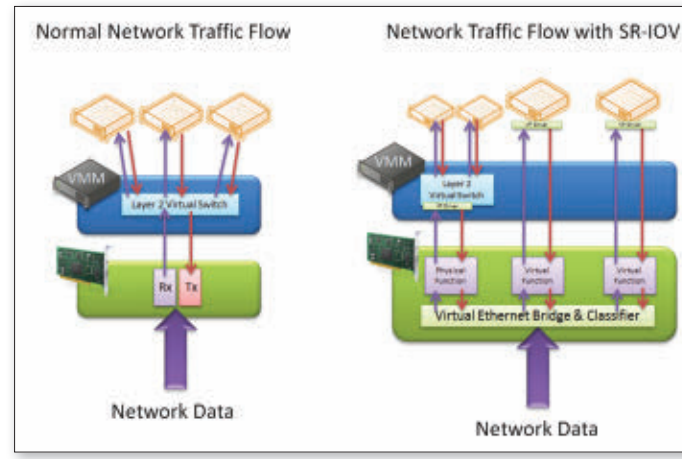


Figure 3: Traffic flow with traditional Hyper-V networking and with SR-IOV

The first time I heard about SR-IOV, I thought, "The whole point of virtualization is to abstract the virtual instance from the underlying hardware for maximum portability. Won't SR-IOV break my mobility because the VM is directly talking to hardware, and therefore I won't be able to Live Migrate to a host that doesn't support SR-IOV?" Hyper-V takes care of this issue. Behind the scenes, the Network Virtualization Service Client (NetVSC) in the VM creates two paths for the VM network adapter (also in the VM). One path is via SR-IOV, and one uses the traditional VMBus path, which uses the Hyper-V switch. When the VM is running on a host with SR-IOV, the SR-IOV path is used and the VMBus is closed. But if the VM is moved to a host without SR-IOV, then NetVSC closes the SR-IOV path and opens the VMBus path, which is transparent to the VM. This means that you don't lose any mobility, even when using SR-IOV.

SR-IOV requires both the server motherboard and the network adapter to support SR-IOV. In addition, the OS must support SR-IOV, which Server 8 does.

Dynamic VMQ

The final enhancement that I want to discuss is the dynamic virtual machine queue. VMQ was actually introduced in Windows Server 2008 R2. VMQ allows separate queues to exist on the network adapter, with each queue being mapped to a specific VM. VMQ removes some of the switching work on the Hyper-V switch: If the data is in a particular queue, then the switch knows that the data is meant for a specific VM. The difference between VMQ and SR-IOV is that the traffic still passes through the Hyper-V switch with VMQ, which presents different traffic queues rather than entire virtual devices. In Server 2008 R2, the assignment of a VMQ to a VM is static. Typically, the assignment is first-come first-served, as each NIC supports a certain number of VMQs.

In Server 8, this assignment is dynamic, so the Hyper-V switch constantly monitors the network streams for each VM. If a VM that was very quiet suddenly becomes busy, then that VM is allocated a VMQ. If no VMQs are available, then the VMQ is taken from a VM that might previously have been busy but is now quiet. Again, network performance benefits.

Cloud-Optimized OS

With Server 8 being Microsoft's cloud-optimized OS and supporting private and public clouds, the changes to networking enable flexibility in VM deployments and mobility while taking advantage of the most recent network hardware improvements. As I stated at the beginning of this article, the OS makes other enhancements to its network capabilities. I'll cover those enhancements in future articles that apply to Hyper-V and non-virtualized scenarios.

InstantDoc ID 141950

John Savill
(john@savilltech.com) is a Windows technical specialist, an 11-time MVP, and an MCITP: Enterprise Administrator for Windows Server 2008. He's currently writing his latest book, *Microsoft Virtualization Secrets* (Wiley).

5 Custom Attributes in Exchange Server 2010 SP2

Find more value in these new multivalued attributes

by Tony Redmond

If you browse the Microsoft article that lists the new features in Microsoft Exchange Server 2010 SP2 ("What's New in Exchange 2010 SP2," technet.microsoft.com/en-us/library/hh529924.aspx), you'll find information about five new multivalued custom attributes. Custom attributes have existed in every version of Exchange since the product was first released in 1996, but they haven't really evolved until now. What are these custom attributes, how are they used, and why has Microsoft chosen to update them now?

Microsoft originally designed custom attributes for use in the Exchange Directory Store (DS) because customers couldn't modify the DS. Different organizations required different things from the directory, and providing a set of custom attributes seemed like a good solution. In addition, when Microsoft launched Exchange, the new product needed to offer the same features as competing products, such as Digital Equipment's ALL-IN-1 Office system, which was the first email server to support customizable attributes in its directory.

Active Directory (AD) somewhat reduced this necessity by supporting a mechanism by which companies can extend the AD schema to add objects and attributes. But in practice, few companies extend AD, largely because they don't want to run the risk that Microsoft will overwrite or otherwise nullify their extensions in a future Windows release. Therefore, custom attributes are as valuable today as they were 16 years ago, even if the technology environment has changed dramatically.

Many Moons Ago

Figure 1 shows the first implementation of custom attributes in Exchange Server 4.0. Of course, 16 years ago, AD was still a blink in the eye of its developers, and Exchange boasted its own DS. The Exchange DS was modeled on the X.500 international standard and provided the basis for the eventual implementation of AD in Windows 2000.

As you can see, Exchange originally allowed administrators to populate as many as 10 custom attributes for a mailbox. This limit existed between Exchange 4.0 and Exchange 5.5 and was increased to 15 custom attributes when Exchange Server 2000 switched over to use AD. The AD schema updates that were required to support Exchange included the addition of the custom attributes. These attributes are simple text fields, each of which can store as many as 1,024 characters. All versions of Exchange since Exchange 2000, including Exchange Online as deployed in Microsoft Office 365, support the same set of 15 attributes for mailboxes, Distribution Groups (DGs—including dynamic DGs), mail-enabled users, and contacts. The current release of Exchange Online in Office 365 supports the new multivalued attributes as well.

Many Varied Uses

Over the years, administrators have found many varied and interesting uses for custom attributes. Common uses include the following:

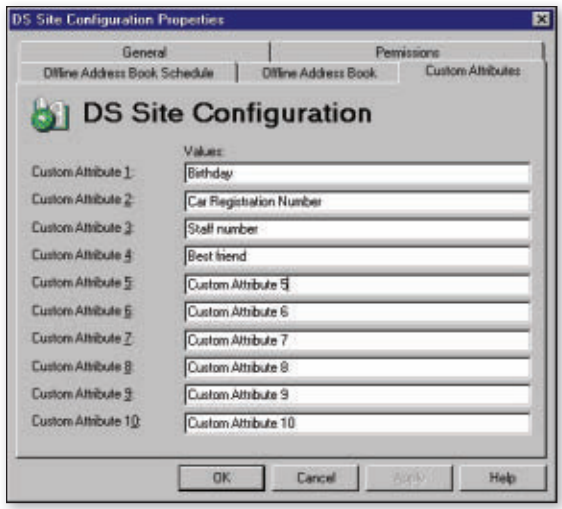


Figure 1: Exchange Server 4.0 custom attributes

- Storing organization-specific information about users, such as badge numbers or location codes.
- Storing other important information that's associated with employees. Social Security numbers and other national taxation identification data are a bad choice; that kind of data should be secured properly and not made available to Exchange administrators. Some companies use these attributes to indicate whether an employee is a manager or occupies some other grade, whereas others use the attributes to store training information.
- Storing information to connect Exchange and other applications. Badge numbers or other employee identifiers are often used to provide a link between Exchange and other applications (e.g., HR systems) and are populated when a mailbox is set up for a new employee.

All this data is essentially single-valued and is typically updated by being overwritten with a new value.

Accessing Custom Attributes

Before the advent of Windows PowerShell in Exchange Server 2007, the typical way for administrators to access custom attributes was through the Exchange Management Console (EMC) or its predecessor. Brave individuals could also use a directory-centric utility such as LDP or ADSIEdit (as Figure 2 shows) to manipulate custom attributes just like any other piece of AD data.

With the Exchange 2010 or Exchange 2007 EMC, you can view custom attributes for an object by selecting the object, viewing its properties, and then clicking the Custom Attributes button to reveal the view that Figure 3 shows.

The Exchange Management Shell (EMS) makes custom attributes more powerful by making it easier to use these attributes to group and filter objects. The EMS is also the only way that Office 365 administrators can access the custom attributes. The Exchange Control Panel (ECP) doesn't currently support viewing or editing the custom attributes.

When you access mailboxes, groups, and contacts through the EMS, the custom attributes are available as CustomAttribute1 through CustomAttribute15. Thus, to get information about the value of all custom attributes for my mailbox, I can run this command:

```
Get-Mailbox -Identity "Tony Redmond" |
  Format-List CustomAttribute*
```

As a more useful example, let's assume that we want to fetch information about all the employees who hold an MCSE qualification. For this example, we'll use CustomAttribute15 to store Microsoft accreditations, and we'll assume that someone has dutifully updated mailboxes with data about MCSE certifications as certification holders have successfully passed exams. To find all the mailboxes, we can run this command:

```
Get-Mailbox -Filter
  {CustomAttribute15 -eq
  "MCSE"}
```

Obviously, the ability to select a group of objects with one command is much better because it provides the basis to further process that group as a whole, such as creating a report about the objects. For instance, after I fetch the collection of mailbox objects that have MCSE stored in CustomAttribute15, I can create a report that lists all the names of the people who are MCSE-qualified in the organization.

New in Exchange Server 2010 SP2

Custom attributes have been a wonderful servant in many situations. However, their single-valued nature is a limitation when you want to store multiple values in a field. For example, "MCSE" is a pretty generic way to describe the accreditation; it's possible to be certified in many different Microsoft technologies. It might be better to store values such as "Exchange," "SQL," "Windows," and so on. This was possible with the existing custom attributes, but adding a new value to an existing list through code is problematic because you essentially must fetch the existing list, add the new value, and then write the new list back into the custom attribute.

The Microsoft solution is a set of five new multivalued attributes. These attributes are included in the AD schema extension that you need to install before deploying Exchange 2010 SP2. The EMC UI hasn't been updated to display the new attributes, so the only way that you can access them is through the EMS. Figure 4 shows how the new attributes appear when

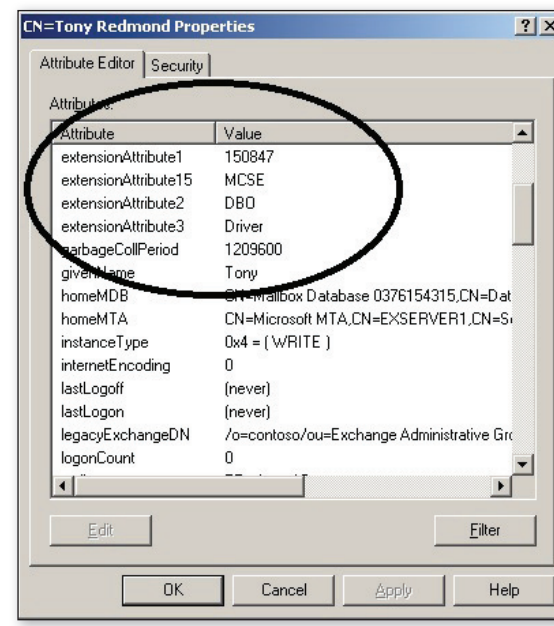


Figure 2: Custom attributes as viewed through ADSIEdit

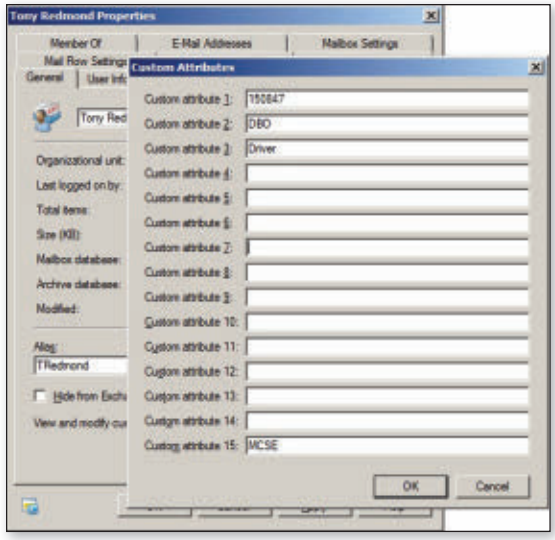


Figure 3: Viewing custom attributes with the Exchange Server 2010 EMC

the EMS lists them with other mailbox attributes.

As you can see, the new attributes are named ExtensionCustomAttribute1 through ExtensionCustomAttribute5. Each attribute can store as many as 1,300 values in a comma-separated list and is available for mailboxes, groups, and contacts. You manipulate the values by using a syntax that's been supported since Exchange 2010 SP1. (See David Strome's blog at blogs.technet.com/b/dstrome/archive/2011/05/29/multivalued-properties-in-exchange-2010.aspx for further details.)

Let's see what happens in some examples. The same code works with both Exchange 2010 SP2 and Exchange Online. In fact, Exchange Online supported multivalued custom attributes well before the release of Exchange 2010 SP2. The change was introduced as part of the Microsoft approach of pushing frequent incremental updates to its Office 365 platform.

First, let's populate a mailbox with some information about the set of technical skills that an individual possesses:

```
Set-Mailbox -Identity
"Tony Redmond"
-ExtensionCustomAttribute1
@("Exchange", "SQL",
"Windows 2008", "Windows 7")
```

I forgot that the user is a Microsoft IIS guru, too. Let's add that value:

```
Set-Mailbox -Identity
"Tony Redmond"
-ExtensionCustomAttribute1
@{add="IIS"}
```

> Exchange automatically indexes data in its custom attributes, so queries against these attributes are very efficient.

A quick check of what we've done so far reveals all the expected values, as Figure 5 shows.

Conversely, if we decide that our subject isn't quite such an IIS pro after all, we can remove the value from the list:

```
Set-Mailbox -Identity "Tony Redmond"
  -ExtensionCustomAttribute1
  @{Remove="IIS"}
```

Note that there's no need to specify the position of the value within the list or to remove the complete list and rewrite it. PowerShell takes care of everything for you. If you want to remove multiple values, simply express them in a comma-separated list. Exchange doesn't support the ability to update position-dependent data in place or to insert a new value into a list in a specific place, so if a value is position-dependent within a list, your code needs to follow the old approach of extracting the previous list, formulating the list with the new data in the correct location, and then updating the attribute with the list of values.

Although I used MCSE qualifications in this example, businesses can apply the same approach to use the new multivalued custom attributes to store lists of items. For example, you can use one attribute to store the ticket numbers of user-reported problems, using values such as Outlook/05-Jan-2012/15154. In this instance, the ticket number is 15154 and the problem was logged with Outlook on January 5, 2012. (Of course, ticket-tracking software is available for this purpose, so you probably won't use the attributes for this specific purpose—but it shows the possibilities.)

Putting Multivalued Attributes to Work

Inputting data is one thing. Using that data in an intelligent fashion is much more interesting.

Dynamic DGs are a great feature of Exchange. After being created, they should need a lot less maintenance than standard DGs, providing that the underlying data is maintained in AD. As the name implies, each time someone sends a message to the group, Exchange dynamically resolves the recipient set by referring

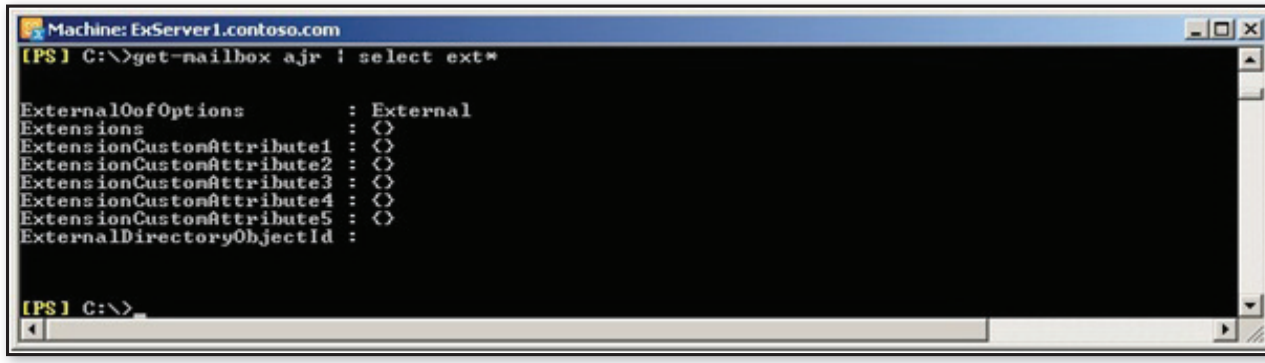


Figure 4: New custom attributes listed for a mailbox

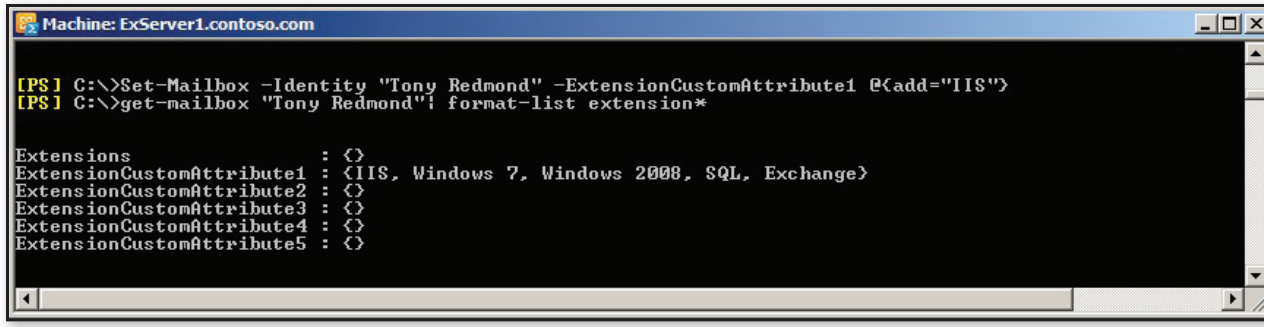


Figure 5: Populating a multivalued attribute

Figure 6: Checking a recipient filter for a dynamic DG

to AD. The magic is accomplished by applying a query against AD to generate a set of recipients that match the criteria expressed in the recipient filter. As long as the data in AD is accurate, dynamic DGs work beautifully and save a heap of administrator time. There's no need to add mailboxes to the recipient list for typical DGs.

The following example creates a new dynamic DG called Exchange Gurus and specifies the recipient filter that Exchange executes to generate the recipient set:

```
New-DynamicDistributionGroup -Name
  "Exchange Gurus" -RecipientFilter
  {(RecipientType -eq "UserMailbox")
  -and (ExtensionCustomAttribute1
  -like "Exchange")}
```

The recipient filter in this example is pretty simple. Essentially, this filter says, "Find all user mailboxes that have the value Exchange stored in ExtensionCustomAttribute1." Recipient filters are stated in OPATH format and can be much more complex than the query that's used in this example. (For more information about how to build OPATH queries for use with Exchange, see the Microsoft article "Creating Filters in Recipient Commands" at technet.microsoft.com/en-us/library/bb124268.aspx.)

The interesting thing is that Exchange automatically indexes data that's held in its custom attributes, so queries against these attributes are very efficient. I use the "-like" operator here to catch values such as "Exchange" and "exchange". You can use the "-eq" operator (a little more efficient than "-like") if you're positive that everyone who populates AD will use the same value.

To view the full recipient filter for a dynamic DG that Exchange uses to search AD, we can use a command such as this:

```
(Get-DynamicDistributionGroup "Exchange
  Gurus").RecipientFilter
```

The bad thing about recipient filters is that you're never quite sure which recipient set will be resolved when Exchange queries AD. Fortunately, it's relatively easy to check. First, we store the recipient filter in a variable; then we feed the filter into the Get-Recipient cmdlet to see what Exchange returns, as the following command shows:

```
$Set = Get-DynamicDistributionGroup
  -Identity "Exchange Gurus"
Get-Recipient -RecipientPreviewFilter
  $Set.RecipientFilter
```

Figure 6 shows the result of this command. As you can see, we've found two well-known Exchange people who like to think of themselves as gurus.

Save Time with Dynamic Distribution

Exchange has included custom attributes for a very long time. The changes introduced in Exchange 2010 SP2 make custom attributes a little easier to manage and a better repository for data that you want to associate with mailboxes. Even better, you can save time by using the new custom attributes as the basis for dynamic DGs.

InstantDoc ID 141780

Tony Redmond
(tony.redmond@windowsitpro.com) is a contributing editor for *Windows IT Pro* and the author of *Microsoft Exchange Server 2010 Inside Out* (Microsoft Press). He blogs about Exchange and related topics at www.windowsitpro.com/go/ExchangeUnwashed.

FEATURE

Hiding Data in Active Directory Part 1

Protecting sensitive data from prying eyes can be quite a challenge

by Guido Grillenmeier

Active Directory (AD) has decent capabilities for setting permissions on objects to allow delegated administration of items such as users, groups, or computers according to any security principal. But when it comes to making specific data visible to only those users who need to see it, the default AD permissions can make the task rather complex.

This multi-part series will discuss AD data-hiding options. These options can be based on typical AD permissions, a special AD permission feature called List Mode, or a little-known option called the confidentiality bit (introduced a few years back with Windows Server 2003 SP1). Windows Server 2008 R2 and Windows Server 2008 have included only minor enhancements with respect to setting permissions on AD data, which I'll also describe.

Before we delve into the details of hiding data in AD, you need a good understanding of the challenge. I'll describe the solution in the future articles in this series.

Understanding the Challenge

The main reason that hiding data in AD is something of a challenge is the various default permissions that are granted in an AD forest. During the design of AD, Microsoft chose to grant numerous read permissions to all authenticated users, for almost all new objects that are created in a forest, instead of locking down the default settings and forcing administrators to grant the appropriate read permissions for the environment. As always, there are pros and cons to both approaches. I would even argue that these less-restrictive default permissions are part of AD's success: Less administrator effort is required to make things work.

Companies are slowly realizing the wealth of default read (and write) permissions that are granted to all the user accounts in their corporate AD implementations. Most companies might want to differentiate between employees, who are allowed to query for all accounts in AD, and external users (e.g., contractors). Also, companies that want to adopt AD as not just a network OS (NOS) directory (which authenticates users to the network) but also as a plain LDAP directory (which is used by other applications) require more control over who can see what. Furthermore, in companies for which delegation of administration is important, the access to and visibility of sensitive accounts is a crucial aspect that needs to be planned carefully. This is certainly the case for outsourcers that might host users from various companies within one AD forest.

By default, all authenticated users in an AD forest are granted explicit read permissions on any organizational unit (OU) that a domain administrator or delegated administrator creates. In this case, any logged-on user can see all objects within any OU in an AD forest. The situation doesn't improve when we look at the default permissions for the different types of AD objects (e.g., a userClass object). As Table 1 shows, authenticated users are granted various read permissions, but SELF (i.e., the user, when accessing his or her own account) has the right to read all properties and to edit many of them.

Table 1: Default Permissions for New User Objects in AD

Security Principal	Default Permissions (Explicit)
Account Operators	Allow: Full Control
Authenticated Users	Allow: Read Permissions, Read General Information, Read Personal Information, Read Web Information, and Read Public Information
Cert Publishers	Allow: Read/Write userCertificate
Domain Admins	Allow: Full Control
Everyone	Allow: Change Password
RAS and IAS Servers	Allow: Read Remote Access Information, Read Account Restrictions, Read Group Membership, Read Logon Information, and Read Public Information
SELF	Allow: List Contents, Read All Properties, Read Permissions, Change Password, Send As, Receive As, Read/Write Personal Information, Read/Write Phone and Mail Options, and Read/Write Web Information
System	Allow: Full Control

Besides these explicit permissions for every new object, various permissions are inherited from parent OUs. Fairly critical default permissions, including Read All Properties for user objects, are granted to the Pre-Windows 2000 Compatible Access group. One of the main challenges is limiting the permissions for authenticated users in such a way that users don't see everything by default. Understanding every annoying detail of AD permissions and how to adjust them now becomes crucial.

Notice I used the term "explicit permissions." Explicit permissions are those that are set directly on objects, as opposed to inherited permissions, which are set on a container object and configured to apply to objects within that container and its subcontainers.

Explicit vs. Inherited Permissions

Both explicit and inherited permissions are needed for an efficient AD authorization model. When a user tries to access an AD object, the security reference monitor must evaluate the list of permissions in ACLs and compare them to the user security identifier (SID) and group SIDs in the security token, to determine whether access should be allowed or denied. To do so, the security reference monitor processes an ACL, starting at the top. When the monitor finds enough access control entries (ACEs) to determine that the access should be denied or allowed, it stops processing the ACL and returns the authorization result (i.e., deny or allow) to the requesting process. The order in which ACEs occur in the ACL determines the effective permissions. Table 2 lists ACE ordering and evaluation priorities.

Deny permissions take precedence over allow permissions, but explicit allow permissions override inherited deny permissions. If child objects inherit an explicit allow permission, that permission also overrides a deny permission that's inherited from further up the OU hierarchy. This means that even if an administrator were to deny access to a certain user attribute (e.g., phone-number) for all external users at the domain head in AD, these permissions generally would be overridden by the default explicit read permissions that are granted to all authenticated users in the forest.

Figure 1 illustrates an example. Although the ExtUsers group is denied read permissions at a top-level OU or at the domain node, some of the sub-OUs still apply the default permissions, which grant authenticated users read access to most objects and attributes. These permissions also apply to newly created objects. And the top-level deny permission can't travel all the way down the tree if it comes across an OU that blocks inheritance of permissions from the parent OU. The future articles in this series will show you how to get past this problematic behavior.

Permission Property Sets

Many AD attributes are grouped into permission property sets. Property sets allow one ACE to grant or deny permissions on an AD object for a collection of attributes. Without property sets, you'd need to apply many separate ACEs for each attribute. A good example of a property set is the Personal Information set. In Server 2008 R2, this set contains 47 attributes, including the user's address and telephone number.

An attribute is defined as belonging to a particular property set by its attributeSecurityGUID property, which matches the rightsGUID property of the property set. Figure 2 shows how the permissions of a property are viewed in the AD security editor and how they're applied to and evaluated for multiple user-object attributes.

Property sets were introduced both to simplify administration and to preserve storage space in AD. The latter shouldn't be underestimated. Every ACE that applies to an object needs to be stored in AD. A permission that's given to a property set is

Table 2: Order of ACE Priority

1	Explicit (non-inherited) deny entries
2	Explicit (non-inherited) allow entries
3	Inherited deny entries
4	Inherited allow entries

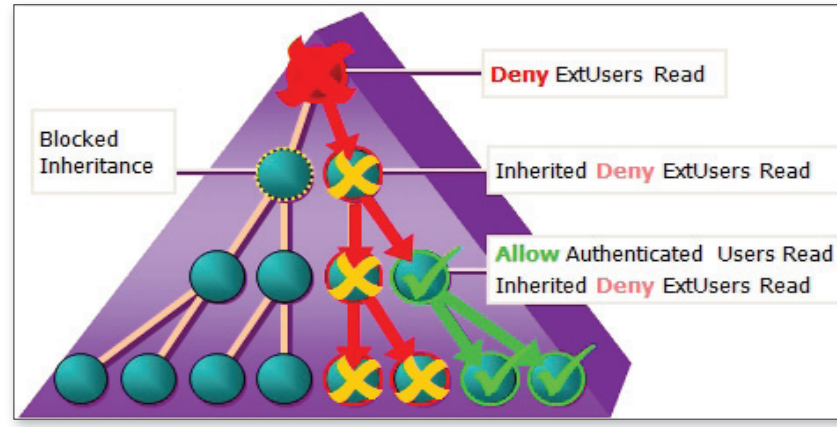


Figure 1: Sample explicit allow permission overriding top-level deny permission

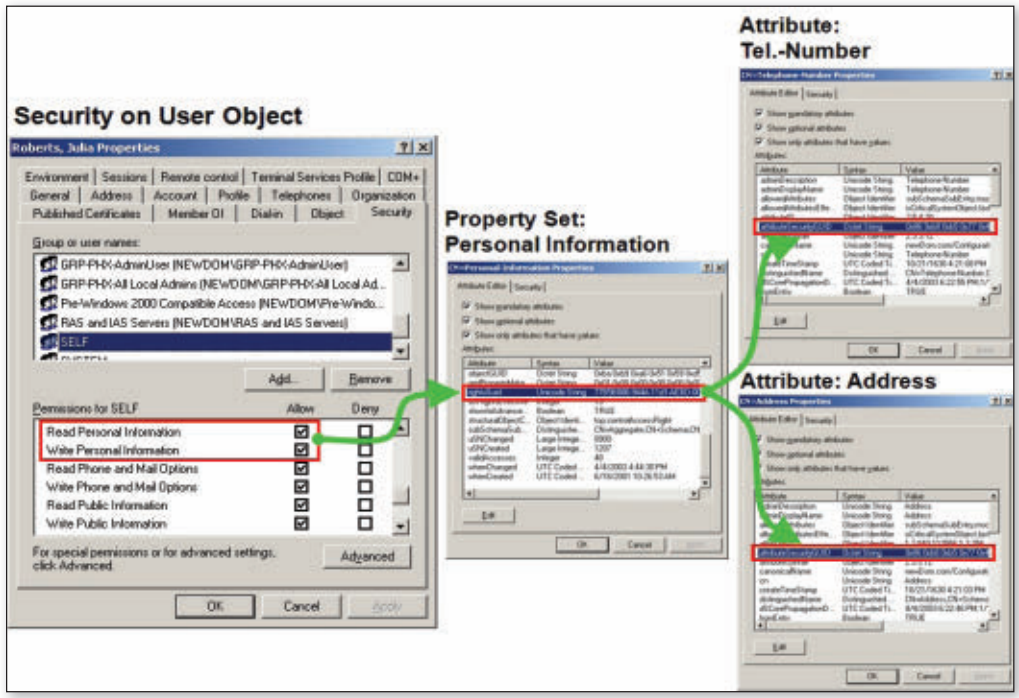


Figure 2: AD permissions can apply to multiple attributes via property sets

both displayed and stored as a single ACE, saving space. Be aware that any attribute in AD can belong to only one property set—an important restriction when it comes to customizing AD security. You can find the definition of all default property sets on the Microsoft Property Sets page at msdn.microsoft.com/en-us/library/ms683990.

Although the majority of property sets are the same across Windows Server versions (as Table 3 shows), an important feature—the ability to edit the default property sets—is available only in Windows 2003 and later. I'll cover the editing of these sets in more detail in the second part of this series.

Table 3 also shows that most of the default property sets still contain the same number of attributes as the initial release of AD. However, a few sets were updated during schema updates, when new features such as LastLogonTimeStamp (in Windows 2003) or ManagedAccounts (in Server 2008 R2) were introduced.

Microsoft Exchange Server also extends the schema through various attributes, some of which are added to the default property sets. But it wasn't until Exchange Server 2007 that Microsoft chose to create new permission property sets that are dedicated to Exchange. In fact, it's rather curious that Exchange doesn't leverage the *Phone and Mail Options* property set, which you would think was meant for a messaging system. Instead, before Exchange 2007, all relevant attributes (120 of them) went into one existing property set: the Public Information property set. This property set also includes all the extensionAttributes, which are expected to store information of public interest only, because authenticated users have default read access to this property. (The Personal Information property set is left untouched by an Exchange installation.)

Of the four property sets to which authenticated users are granted default read permissions on user objects (i.e., General Information, Personal Information, Web Information, and Public Information), the Personal Information property set is usually of greatest interest to administrators who want to hide access to specific account data. This set contains potentially sensitive data, such as the employee's home phone or home address. Although companies might not feed this data into AD automatically, every user can do so through the default permissions that are granted to the SELF security principal. Figure 3 lists the 47 attributes that belong to the Personal Information set in Server 2008 R2.

So, why are property sets important when discussing hiding data in AD? It's quite simple. Take another look at Table 1, which lists the default permissions

Table 3: Default Property Sets in AD

Property Set Name		Number of Attributes in Property Set			
Common Name	Display Name	Win2K	Windows 2003 and 2003 R2	Server 2008	Server 2008 R2
DNS-Host-Name-Attributes	DNS Host Name Attributes	N/A	2	2	2
Domain-Other-Parameters	Other Domain Parameters (for use by SAM)	N/A	7	7	7
Domain-Password	Domain Password & Lockout Policies	8	8	8	8
Email-Information	Phone and Mail Options	0	0	0	0
General-Information	General Information	12	13	13	13
Membership	Group Membership	1	2	2	2
Personal-Information	Personal Information	41	41	46	47
Public-Information	Public Information	34	37	44	44
RAS-Information	Remote Access Information	9	9	9	9
User-Account-Restrictions	Account Restrictions	4	5	6	6
User-Logon	Logon Information	9	12	12	12
Web-Information	Web Information	2	2	2	2

assistant	otherPager
c	otherTelephone
facsimileTelephoneNumber	pager
homePhone	personalTitle
homePostalAddress	physicalDeliveryOfficeName
info	postalAddress
internationalISDNNumber	postalCode
ipPhone	postOfficeBox
l	preferredDeliveryMethod
mobile	primaryInternationalISDNNumber
msDS-FailedInteractiveLogonCount	primaryTelexNumber
msDS-FailedInteractiveLogon-CountAtLastSuccessfulLogon	registeredAddress
msDS-HostServiceAccount	st
msDS-LastFailedInteractive-LogonTime	street
msDS-LastSuccessfulInteractive-LogonTime	streetAddress
msDS-SupportedEncryptionTypes	telephoneNumber
mSMQDigests	teletexTerminalIdentifier
mSMQSignCertificates	telexNumber
otherFacsimileTelephoneNumber	thumbnailPhoto
otherHomePhone	userCert
otherIpPhone	userCertificate
otherMobile	userSharedFolder
	userSharedFolderOther
	userSMIMECertificate
	x121Address

Figure 3: Attributes of the Personal Information property set

that are granted to every new user object in AD. You'll see that four explicit allow read permissions for authenticated users (i.e., General Information, Personal Information, Web Information, and Public Information) are granted to property sets. Add this to the higher priority of explicit allow permissions over inherited deny permissions, and it becomes clear that hiding the data of attributes that are part of a property set is no simple task. You can't just set a deny permission for an object attribute at the OU level and force inheritance to the respective objects. That's why administrators must have a good understanding of property sets and the attributes that belong to them, to fully understand the effect of permissions that are granted or denied to specific attributes in AD.

Note that using third-party tools to manage AD permissions usually helps only when granting new permissions. However, hiding data often requires removing existing permissions that are granted by default. These permissions need to be adjusted in the native permissions of the directory—only after being validated and tested in a proper test lab, of course.

When Is Hiding Data Necessary?

This article would certainly have a different focus if the default read permissions for authenticated users in AD weren't as pervasive as they are. By now, it should be clear that the challenge of hiding data in AD is closely related to three things:

- the default read permissions that are granted to new AD objects
- the priority of inherited permissions during the ACL evaluation process
- the grouping of AD attributes into property sets

Most OU structures are designed to group objects of a similar type or location into one OU. Figure 4 shows how a company might have one OU for managing objects in Atlanta (ATL) and another for managing objects in Phoenix (PHX). Note that both location-level OUs have sub-OUs to further subdivide object types for each location. These divisions allow the delegation of different administrative rights or the application of different Group Policy policies.

Also notice the special sub-OU called Local Admins in Figure 4. This sub-OU is meant to hold special account data for the delegated administrators of the location. To protect these users from potential misuse or Denial of Service (DOS) attacks, it's a good idea to hide the Local Admins OUs from end users.

Another reason for hiding users or complete OUs is to prevent other users knowing of their existence in AD. This capability can be important in sensitive environments such as financial institutions, government agencies, or outsourcing companies, in which each top-level OU represents a different customer, each of which should be able to see only that customer's objects.

There are also technical reasons to hide data in AD, especially when it becomes important to limit delegated administrators' ability to link AD objects. When you add a user as a member of a group, you link that user to the group. You aren't actually editing the user object properties, only the group's membership attribute (the forward link). In our previous sample OU structure, suppose that a delegated administrator has all the required permissions to manage groups and users in Phoenix (OU PHX) but not in Atlanta (OU ATL). That administrator, by default, can still add users from the ATL OU (or any other place in the AD forest) to groups in OU PHX. Companies usually accept this issue, which also offers an easy way to establish cross-boundary access to shared resources, such as file servers, or to provide vacation coverage for site admins.

However, in ISP scenarios and other sensitive environments, administrators often must not be able to add users from outside their scope of responsibility (i.e., outside the OU or OUs that they manage) to groups that they do manage. In such cases, you also need to hide users that are outside the OUs that a delegated administrator manages so that the administrator can't add those users to their groups or to any other linked attributes, such as to the manager attribute of a user or the managedBy attribute of objects such as printers, groups, or OUs.

Finally, companies might need to hide data that's stored in specific attributes of different types of objects in AD, instead of hiding the complete object. This need depends on the sensitivity of the data. For example, if a company stores users' employee numbers in AD, it might want to hide that information to all users who aren't in HR. Similarly, the company might want to restrict access to the home phone

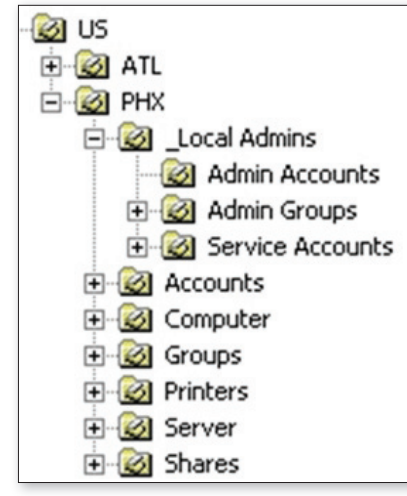


Figure 4: Sample OU structure

Learning Path

Check out these articles for more general information about Active Directory:

"Troubleshooting Active Directory Replication," InstantDoc ID 129333

"Active Directory Replication In Depth," InstantDoc ID 135815

"Active Directory Replication Topology," InstantDoc ID 140895

"Delegating Privileges in Active Directory," InstantDoc ID 129156

"What's New in Windows Server 8 Active Directory," InstantDoc ID 140571

"Identity as a Service and the Future of Active Directory," InstantDoc ID 136210

"Avoid Active Directory Mistakes in Windows Server 2008," InstantDoc ID 142023

Check out these articles for more information about Active Directory and security:

"Advanced Active Directory Security," InstantDoc ID 125777

"4 Challenges of Auditing AD Users and Groups," InstantDoc ID 141463

"How-To: Use LDAP Over SSL to Lock Down AD Traffic," InstantDoc ID 141170

"Active Directory Rights Management Services Secure Collaboration," InstantDoc ID 140326

"The Care and Feeding of the Active Directory Security Access Token," InstantDoc ID 139827

number attribute. More often, companies have added their own attributes in the AD schema to store additional information for other applications. Common schema extensions include attributes for cost centers or special application-specific roles, or even attributes that store token IDs to support other authentication methods that use AD as an LDAP server. Many of these special attributes aren't meant to be seen by end users or lower-privileged administrators, such as Help desk operators. The information in these special attributes could pose a risk to the company if it falls into the wrong hands.

Table 4: Options for Configuring AD Permissions for Hiding Data

Permission Option	Scope	OS Version	Short Description
Using "Normal" permissions on AD objects and attributes	Objects and attributes	Win2K; Windows 2003; Server 2008	Sensibly restricting normal read permissions in AD already gives an administrator great control over the visibility of objects and attributes.
Enabling List Object Mode in Forest	Objects	Win2K; Windows 2003; Server 2008	This special mode lets you differentiate the visibility of single objects within containers such as OUs.
Adjusting the default security of objects in AD	Objects and attributes	Win2K; Windows 2003; Server 2008	This option is valid for new objects only. The permissions that are applied to objects at creation in AD can be adjusted.
Adjusting the built-in property sets	Attributes	Windows 2003; Server 2008	The set of attributes that belong to the built-in property sets can be adjusted. This option isn't possible in Win2K.
Using the confidentiality bit	Attributes	Windows 2003 SP1; Server 2008	In Windows 2003 SP1 and later, this option can hide specific attributes from users, even when general access to read all attributes of an object is granted (similar to List Mode, but at the attribute level).

In summary, these are the most common reasons for hiding data in AD:

- to protect administrative accounts from misuse and DOS attacks
- to hide the existence of specific objects for legal reasons
- to honor least privilege for special administrative tasks, such as ensuring that delegated group administrators can change membership for users within their own administrative scope only
- to ensure that sensitive data within attributes is disclosed to authorized users only

Options for Hiding Data

In general, the goal when hiding data in AD is to hide data from unauthorized users and make it accessible only to those who are specifically allowed to view it, via membership in an appropriate security group, for example. With this goal in mind, the preferable solution is to limit access (i.e., default deny) to objects or attributes by ensuring that only specific security principals (e.g., security groups) are granted access to them, rather than first granting general access (i.e., default allow) to an object (e.g., to all authenticated users) and then trying to deny access to unauthorized users. We also need to differentiate which data is supposed to be hidden in the first place: the whole object, or just specific attributes of an object?

Table 4 lists the main options that are available to hide data in AD, including the scope (objects or attributes) and the OS version that supports the respective option. In reality, administrators often need to combine different permission configuration options to reach their AD data-hiding goals.

As with most things, understanding the problem before designing an appropriate solution is crucial. This article describes why hiding data in AD is a challenge in the first place, gives examples for when you might need to do so, and helps you understand the available options for solving this challenge. The future articles in this series will explain, in detail, how to use these options to hide objects in AD or data that's stored in specific attributes of AD objects. Part 2 will discuss how to use normal permissions on AD objects and attributes, enable List Object Mode in a forest, or adjust the default security of objects in AD. Part 3 will cover adjusting the built-in property sets. Finally, Part 4 will explain how to use the confidentiality bit and how to configure the filtered attribute set to adjust which attributes are replicated to read-only domain controllers (RODCs).

InstantDoc ID 142135

Guido Grillenmeier
(guido.grillenmeier@hp.com) is a chief engineer within the Enterprise Services Group at HP. He is a Microsoft Directory Services MVP, a Microsoft Certified Architect, and the coauthor of *Microsoft Windows Security Fundamentals* (Digital Press).

Power Through Registry Searches with PowerShell

Use this script for faster results

by Bill Stewart

Anyone who has been responsible for managing Windows machines for any length of time will be familiar with the registry. The registry was originally created as a way for the OS to store information about file types. But starting in Windows NT 3.1 and Windows 95, the registry became the standard place in which the OS and applications can quickly store and retrieve configuration information. Windows 95 introduced regedit, the standard GUI registry-editing tool; Windows NT provided another GUI registry editor, regedt32, which supported more registry types than regedit did. Windows NT 4.0 and Windows 2000 provided both editors. Starting in Windows XP, Microsoft upgraded regedit to support the same data types as regedt32, making the latter editor obsolete.

Regedit is an extremely useful tool, but searching for data isn't one of its strong suits. Regedit's Find feature, which Figure 1 shows, is basic: Press Ctrl+F, enter a text string, select any of the four check boxes, and click Find Next. Pressing F3 to repeat the search quickly becomes tedious when there are many matches.

I decided to rectify this weakness by writing a Windows PowerShell script, Search-Registry.ps1, which can search the registry more flexibly than regedit. Search-Registry.ps1 improves on regedit's Find feature in four ways:

- The script searches by using regular expressions.
- It can search the registry on remote computers.
- It can limit the number of returned search results.
- It outputs objects than can be filtered, sorted, exported to comma-separated value (CSV) files, and so on.

Many PowerShell-savvy readers will note that PowerShell provides registry "drives" (e.g., HKLM) for accessing the registry. However, these drives work only on the local computer, not on remote systems. I also considered PowerShell remoting. But remoting requires that PowerShell 2.0 or later be installed and enabled on all remote machines—a scenario that doesn't occur by default.

Introducing Search-Registry.ps1

The Search-Registry.ps1 script's command-line syntax is as follows:

```
Search-Registry [-StartKey] <String> [-Pattern] <String> [-MatchKey] [-MatchValue]
[-MatchData] [-MaximumMatches <n>] [-ComputerName <String[]>]
```

The -StartKey parameter specifies the registry key location from which to start searching. This is equivalent to selecting a starting location in regedit's left pane before pressing Ctrl+F. The -StartKey parameter string uses the format

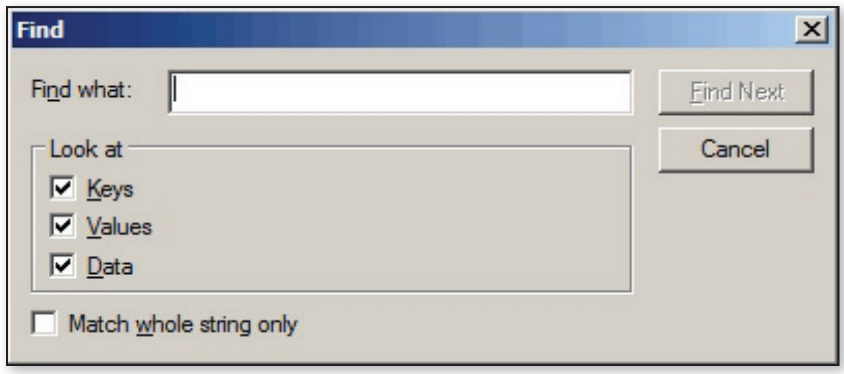


Figure 1: Regedit's Find dialog box

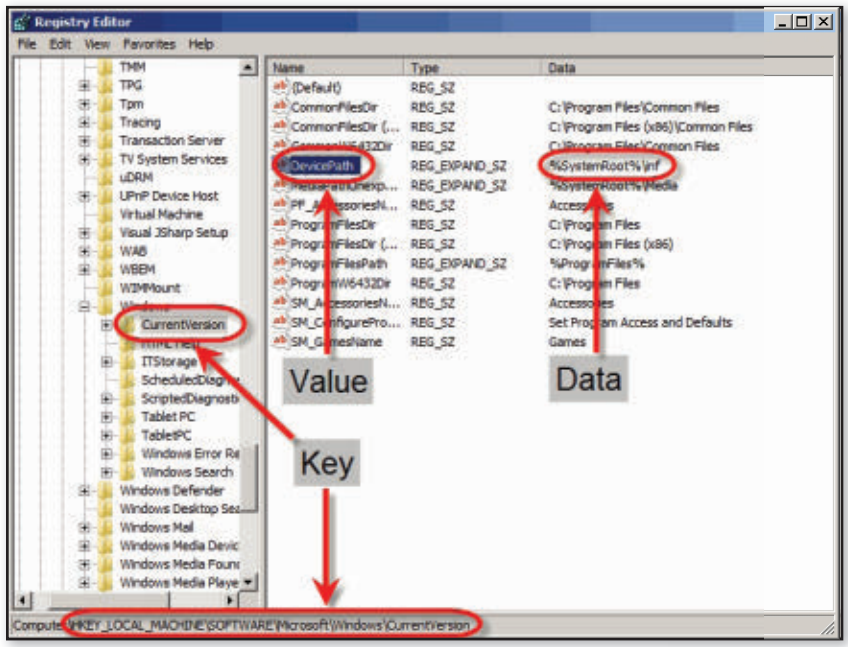


Figure 2: How items in the script correspond with items in the registry

```
subtree:\key
```

where *subtree* is either the abbreviated PowerShell drive name or the full subtree name, as seen in regedit:

- HKCR or HKEY_CLASSES_ROOT
- HKCU or HKEY_CURRENT_USER
- HKLM or HKEY_LOCAL_MACHINE
- HKU or HKEY_USERS

The colon (:) after the subtree name is optional. The *key* specifies where to start searching. If you omit the key or use a single backslash character (\), the script searches the entire subtree. For example, the following strings are all equivalent when used with the -StartKey parameter:

```
HKLM\SOFTWARE
HKLM:\SOFTWARE
HKEY_LOCAL_MACHINE\SOFTWARE
```

The -StartKey parameter is designated to be in position 1, so as long as you specify its argument first on the command line, the -StartKey parameter name is optional. If the -StartKey parameter argument string contains spaces, then surround the string with quotation marks (").

The -Pattern parameter specifies the regular expression pattern that you want to find. The -Pattern parameter is designated to be in position 2, so as long as you specify its argument second on the command line, the -Pattern parameter name is optional. If the -Pattern parameter argument string contains spaces, use quotation marks as appropriate. The regular expression pattern is not case-sensitive. For more information about constructing a regular expression pattern, enter the command

```
help about_Regular_Expressions
```

at the PowerShell command prompt.

The -MatchKey, -MatchValue, and -MatchData parameters specify the kinds of matches that the script should find. These parameters correspond to the Keys, Values, and Data check boxes in regedit's Find dialog box, as Figure 1 shows. Figure 2 illustrates how these items correspond to items in the registry. I decided to stick with these names instead of the new names (i.e., path, property, value) that PowerShell uses in its registry provider so that the script uses the same terms that the regedit Find dialog box uses. You must specify at least one of these three parameters, although you can specify more than one. -MatchKey matches subkey names, -MatchValue matches registry value names, and -MatchData matches the values' data.

The -MaximumMatches parameter specifies the maximum number of results per searched computer. The default value is 0, which returns the maximum number of possible matches. This parameter is useful when searching the registry on remote computers; you can use it to minimize the amount of network traffic.

The -ComputerName parameter searches the registry on the specified computer or list of computers. You can specify one computer name or an array of names. This parameter supports pipeline input. The default is to search the local computer's registry.

Search-Registry.ps1 outputs objects that contain the properties that Table 1 lists. Figure 3 shows a sample Search-Registry .ps1 command in a PowerShell console window. The script that Figure 3 shows

Table 1: Search-Registry.ps1 Output Object Properties

Property	Description
ComputerName	This is the computer on which the match occurred.
Key	This is the key name (see Figure 2). If you use -MatchKey and the key name matches, then the Value and Data properties will be empty.
Value	This is the registry value (see Figure 2).
Data	This is the registry data (see Figure 2).

Learning Path

More PowerShell scripting articles from Bill Stewart:

"4 Challenges of Auditing AD Users and Groups," InstantDoc ID 141463

"Use PowerShell to Run Programs on Remote Computers," InstantDoc ID 141270

"How-To: Use PowerShell to Report on Scheduled Tasks," InstantDoc ID 140978

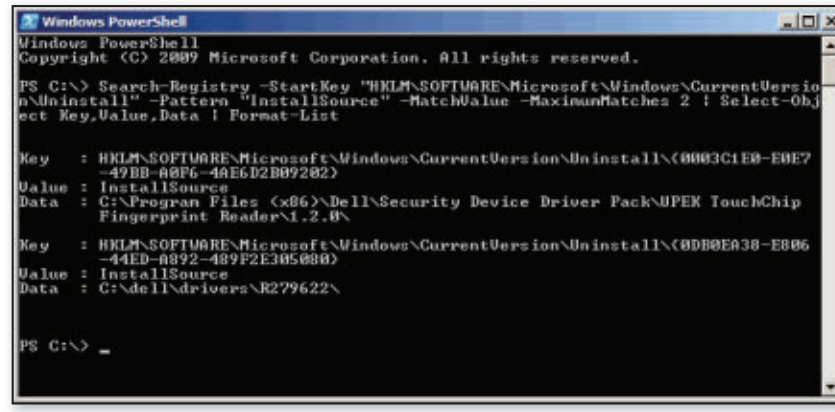


Figure 3: Running Search-Registry.ps1

sends its output to Select-Object to select only the Key, Value, and Data properties (the ComputerName property isn't needed because this command searches the local computer's registry). Select-Object then sends this output to Format-List. The list contains only two matches because of the specified -MaximumMatches parameter.

Depending on the OS, some registry locations might be inaccessible (e.g., because of insufficient permissions). These registry locations will output errors when Search-Registry.ps1 tries to access them. To ignore these errors, specify the -ErrorAction SilentlyContinue parameter in the script's command.

How Does It Work?

Search-Registry.ps1 uses the *begin* and *process* scriptblocks because it supports pipeline input. The begin scriptblock contains the script's initialization code: global variable declarations, parameter validations, and function definitions. The process scriptblock iterates each computer name that's passed to the script and passes the computer name to the search-registry2 function.

The search-registry2 function uses the OpenRemoteBaseKey static method of the .NET Microsoft.Win32.RegistryKey class to open the subtree that you request at the command line, and then passes each computer name to the search-registrykey function. The search-registrykey function searches recursively for the regular expression pattern in a registry location (i.e., it starts at a specified key and also searches in all subkeys of that key).

Sample Commands

Let's take a look at some real-world examples of how you might use Search-Registry.ps1. Keep in mind that although the code in these examples wraps because of space, you would enter them all on one line in PowerShell.

```
Search-Registry -StartKey HKCR -Pattern
  "Word\.Document\.\d" -MatchKey
```

This command searches the local computer's registry, starting at HKEY_CLASSES_ROOT, for the pattern "Word\.Document\.\d". In regular expressions, a period (.) matches any character; a backslash (\) means "interpret the next character literally." Therefore, "\." means ".". A backslash followed by the letter d (\d) indicates "any decimal digit," so this search finds registry subkeys that are named Word.Document.*n* (where *n* is a number). If this command returns a match, then there's probably an application on the local system that can open Microsoft Word documents.

```
Search-Registry -StartKey HKLM -Pattern
  $ENV:USERNAME -MatchData
```

This command searches HKEY_LOCAL_MACHINE on the local computer for any registry data that contains the current user name.

```
Search-Registry -StartKey HKLM\
  SOFTWARE\Microsoft\Windows\
  CurrentVersion\Policies\System
  -Pattern EnableLinkedConnections
  -MatchValue
```

This command determines whether the EnableLinkedConnections registry value is configured on the local computer. (To find out why you might want to search for this value, see the Microsoft article "Programs may be unable to access some network locations after you turn on User Account Control in Windows Vista or in Windows 7" at support.microsoft.com/kb/937624.)

```
Get-Content Computers.txt |
Search-Registry HKLM\SOFTWARE\
  Microsoft\Windows\CurrentVersion\
  Policies\System -Pattern
  EnableLinkedConnections -MatchValue |
Export-CSV C:\Reports\
  EnableLinkedConnections.csv
  -NoTypeInformation
```

This command is the same as the previous one, except that Search-Registry.ps1 searches for the registry value on the computers that are listed in the file Computers.txt and creates a CSV report.

Hassle-Free Registry Searching

Searching for information in the registry no longer needs to be a tedious exercise. Hitting F3 a couple hundred times in regedit can be a thing of the past. The next time you need to search the registry, open a PowerShell command window and use Search-Registry.ps1 instead.

InstantDoc ID 141799

Bill Stewart
(bstewart@iname.com) is a scripting guru who works in the IT infrastructure group at Emcore in Albuquerque, New Mexico. He has written numerous articles about Windows scripting, is a moderator for Microsoft's Scripting Guys forum, and offers free tools on his website at westmesatech.com.

BitLocker Administration and Monitoring

Simplify BitLocker provisioning, reporting, and recovery

by Jan De Clercq

Windows BitLocker Drive Encryption offers volume-level data encryption for data stored on Windows client and server platforms. BitLocker protects that data when the Windows systems are offline (i.e., when the OS is shut down) and can prevent data breaches such as the theft of confidential data on laptop computers.

The first version of BitLocker, which shipped with Windows Server 2008 and Windows Vista, protected only one volume: the OS drive. In Server 2008 and Vista SP1, Microsoft added support for BitLocker protection of different volumes, including local data volumes. In Server 2008 R2 and Windows 7, Microsoft added BitLocker support for removable data volumes—memory sticks and external data drives—a feature that Microsoft refers to as BitLocker To Go.

BitLocker is a valuable security add-on to the Windows OS. BitLocker can help organizations to save money because they don't need to invest in special third-party disk-encryption software. But organizations are often reluctant to implement BitLocker because of its deployment and management complexity.

To tackle these issues, Microsoft has released Microsoft BitLocker Administration and Monitoring (MBAM), part of the Microsoft Desktop Optimization Pack (MDOP). This article provides an overview of MBAM and its architecture and explains how the tool can ease BitLocker deployment and management pains by providing better provisioning, recovery, and reporting capabilities.

MBAM Architecture

MBAM is a client/server application that consists of the MBAM client agent and a set of MBAM server components. Microsoft currently (at press time) provides 32-bit and 64-bit versions of the MBAM client for the Windows 7 platform only. The MBAM client agent enforces BitLocker settings on Windows 7 clients, gathers BitLocker recovery passwords and compliance and configuration data, and forwards this data to the central MBAM server.

The 64-bit MBAM server consists of five components that can be hosted on one server or spread across servers:

- the administration and monitoring server
- the compliance and audit database
- the recovery and hardware database
- the compliance and audit report templates
- the MBAM Group Policy Object (GPO) template

The MBAM server installation wizard lets you select which components you want to install on which machine, as Figure 1 shows. Microsoft recommends using a three- or five-computer configuration when deploying MBAM in your production environment. With the five-machine

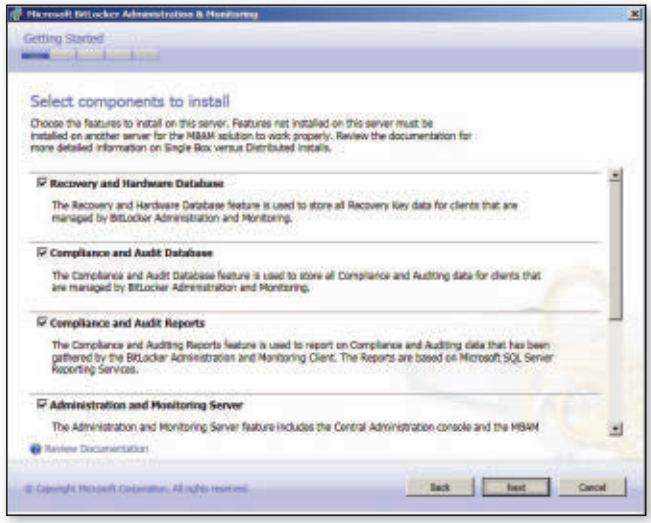


Figure 1: MBAM server installation wizard

configuration option, each MBAM component is deployed on a different machine. In the three-machine configuration option, the recovery and hardware database, the compliance and audit database, and the compliance and audit reports components are co-located on one server.

The MBAM administration and monitoring server component hosts the web-based management console and data collection web services. The component builds on the Server 2008 IIS Web Server role. Administrators use the management console to generate reports, check client BitLocker compliance status, and access BitLocker recovery passwords. When you install the MBAM administration and monitoring server, you'll notice that it automatically adds five MBAM-specific security groups to Active Directory (AD). You can use these groups to fine-tune MBAM administrative delegation.

As an optional subcomponent of the administration and monitoring server, you can install the MBAM hardware capability manager. This subcomponent allows the MBAM administrator to define which client hardware types can run BitLocker and should be centrally controlled through the MBAM BitLocker GPO. After the hardware capability manager is enabled, all MBAM clients use its centrally defined hardware capability list to determine whether the client computer can support BitLocker. The MBAM clients then pass this information to the central MBAM reporting server.

The MBAM administration and monitoring server component links to two Microsoft SQL Server databases: a compliance and audit database, and a recovery and hardware database. The compliance and audit database stores the BitLocker compliance data of all MBAM-enabled client computers. The recovery and hardware database stores the BitLocker recovery passwords. Both databases require different SQL Server 2008 R2 database instances that can be co-located on a single SQL Server 2008 R2 machine (as in the three-machine MBAM configuration option).

The MBAM server also includes a set of compliance and audit report templates that can be used in conjunction with SQL Server Reporting Services (SSRS). Compliance and audit reports can be accessed from the web-based MBAM management console or directly from the SSRS server.

Last but not least, the MBAM server comes with an MBAM GPO template for extending the central control of clients' BitLocker configuration. Administrators can leverage this template (an *.admx file) from the Group Policy Management Console (GPMC) or the Advanced Group Policy Management (AGPM) console.

Easier Provisioning

After you deploy the MBAM server-side infrastructure and enable BitLocker on your Windows 7 clients, using MBAM is a two-step process. First, you must deploy the MBAM client to your user workstations. Then, you must configure the MBAM-specific GPO settings.

The MBAM client is a standard Windows Installer (*.msi) file that you can deploy by using any software-distribution tool. You can leverage the GPO Software Installation feature, System Center Configuration Manager (SCCM) 2007 or 2012, or similar tools.

When the MBAM client is successfully deployed on a Windows 7 client, you'll notice that a new service—the BitLocker Management Client Service—is set to automatically start in the system's Services list. The Control Panel also holds a new applet, Windows BitLocker Administration, which lets users check the BitLocker status of their computers' volumes and easily change their BitLocker unlock PIN or password. Windows BitLocker Administration can also be accessed by clicking the corresponding entry from a BitLocker-protected drive's context menu in Windows Explorer.

The MBAM client also enables a new wizard that lets users easily protect their computers by using BitLocker. If the central MBAM GPO specifies that a computer is to be protected by using BitLocker, then the MBAM client prompts the user to enable BitLocker, as Figure 2 shows. When the user agrees to do so, MBAM starts a wizard that walks the user through the encryption process. The wizard can prompt the user for a PIN and can cover Trusted Platform Module (TPM) configuration, depending on the content of the central MBAM GPO.

Another interesting feature of the MBAM client is that it lets standard users initiate BitLocker volume encryption. (Legacy BitLocker requires administrator privileges to do so.) After you deploy the client agents, you can centrally configure them by using the new MBAM GPO settings. Before you can use these GPO settings, remember that you must have installed the administrative template that's included in the MBAM server installer on your GPO management workstation.

MBAM adds about 20 new BitLocker-related GPO settings in the \Computer Configuration\Administrative Templates\Windows Components\MDOP MBAM (BitLocker Management) GPO container, as Figure 3 shows. Note that this new container is different from the BitLocker Drive Encryption container. The new GPO settings include settings to configure the MBAM client, the addresses of the password recovery and reporting MBAM server components, and the BitLocker encryption rules for fixed, OS, and removable drives.

The previous paragraphs explained how you can use MBAM to provision BitLocker after client computers have been distributed to users. Besides this provisioning method, there's another option for

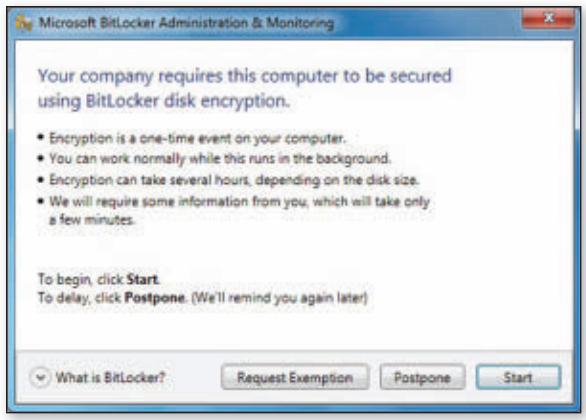


Figure 2: MBAM client/user interaction

organizations in which new computers are centrally configured before they're distributed to users. In such a situation, you can encrypt each computer before user data is written to it. To do so, use the standard Windows 7 deployment tools.

Simpler Recovery

BitLocker requires a solid recovery strategy and forces the user to define a recovery method during BitLocker setup. These requirements allow users to regain access to their data when the encrypted drive cannot be accessed. On an OS drive, you need a recovery method when users forget their PINs, users lose the USB token that holds the BitLocker startup key, or the TPM registers integrity changes to the system files. For data drives, you need a recovery method when users forget their passwords or lose their smart cards. Also, if a protected data drive is configured for automatic unlocking, you need a recovery method if the auto-unlock key that's stored on the computer is accidently lost (e.g., after a hard disk failure or reinstallation).

MBAM provides important enhancements to the recovery password–based recovery method. BitLocker supports three recovery methods:

- a recovery password
- a recovery key
- a data recovery agent (DRA)

A recovery password is a 48-bit numerical password that is generated during BitLocker setup. You can save the recovery password to a file, you can print it, or it can be automatically saved in AD. For more information about BitLocker recovery methods, see the recovery strategy section in "Deploy BitLocker in Your Organization the Right Way" (March 2011, InstantDoc ID 129258).

MBAM provides a better alternative to storing the BitLocker recovery password in AD. Organizations seldom want to store BitLocker recovery data in AD because doing so implies that all AD administrators can access the data, indirectly or directly. And in AD, the recovery data is stored in clear text. MBAM stores BitLocker recovery data in a separate and encrypted SQL Server database.

You can access the MBAM password recovery page by navigating to the default MBAM administration and monitoring page from your browser. Then, in the left navigation panel, select Drive Recovery, as Figure 4 illustrates. You must then enter the AD user ID and domain, a reason why the user is asking for the recovery password, and the first eight characters of the recovery password ID. The latter is displayed after the user or Help desk operator reboots the client machine in drive recovery mode. After you click Submit, MBAM retrieves the recovery password from its recovery database. The administrator or Help desk operator can then pass the password to the user, who can enter the password on the client to unlock the computer's drive.

An important detail: MBAM also enables single-use recovery passwords. MBAM automatically resets the recovery password for the drive so that the old password can't be used again. This action can prevent unauthorized users from gaining access to a BitLocker-protected hard drive when they get access to a previously used recovery key.

Better Reporting

Administrators who've struggled with the creation of BitLocker reports on their client machines will certainly welcome MBAM's reporting capabilities. You can use the MBAM reports to quickly determine whether your Windows 7 clients are compliant with your BitLocker policy. For example, when a user laptop that contains corporate data is stolen or lost, MBAM reports let you rapidly determine whether the loss represents a risk: You can use the MBAM compliance report to see whether the user's laptop had BitLocker enabled on its data volumes.

By default, MBAM provides these reports in the MBAM management console:

- enterprise compliance report
- computer compliance report
- hardware audit report
- recovery audit report

In addition to these four default reports, you can create custom compliance reports by using SSRS tools.

The enterprise compliance report tells you the BitLocker compliance status of all clients in your organization. It shows which machines are compliant, noncompliant, and exempt from the BitLocker policy. The computer compliance report lets you search by computer or username and shows whether a specific computer or user's computers are compliant with BitLocker policy. When a laptop is lost, you can use this report to quickly determine its BitLocker status. The recovery audit report shows who has accessed or tried to

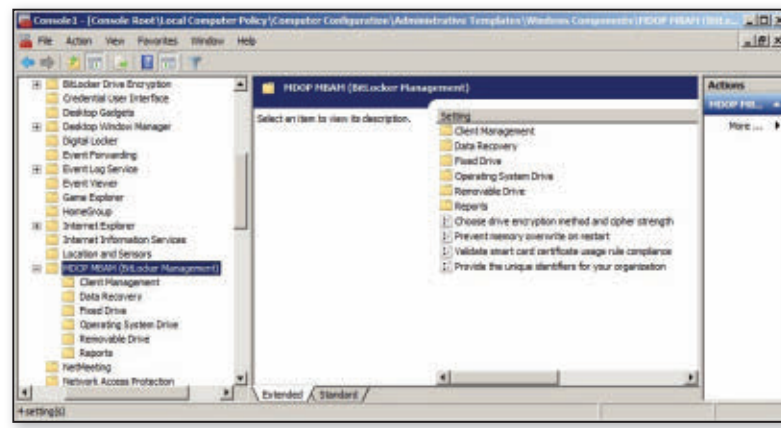


Figure 3: MBAM GPO settings

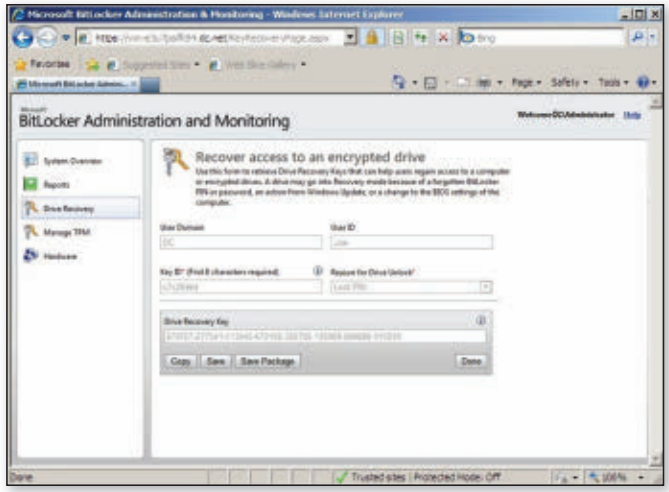


Figure 4: MBAM drive-recovery webpage

access recovery password information in the MBAM key recovery database. Finally, the hardware audit report indicates who has changed the hardware compatibility list and when the MBAM client discovers new hardware. This report is useful only when you've also installed and use MBAM hardware compatibility checking in your organization.

You can access the default reports by navigating to the default MBAM administration and monitoring page from your browser. In the left navigation panel, select Reports and then the specific report that you want to generate. MBAM displays the resulting report on a web page. You can also save the results in another format (e.g., Word document, Excel spreadsheet). To generate reports, you must be a member of the MBAM Report Users AD group on the server or servers on which the MBAM administration and monitoring server and compliance status database are installed.

Taking BitLocker Management to the Next Level

With MBAM, Microsoft provides a tool that administrators will greatly appreciate. MBAM's ability to easily create BitLocker usage reports and to quickly recover BitLocker recovery passwords from a SQL Server database (not in AD) are especially valuable BitLocker additions.

InstantDoc ID 141818

Jan De Clercq
(jan.declercq@hp.com) is a member of HP's Technology Consulting IT Assurance Portfolio team. He focuses on cloud security, identity and access management, architecture for Microsoft-rooted IT infrastructures, and security of Microsoft products. He's the co-author of *Microsoft Windows Security Fundamentals* (Digital Press).

Best Practices for SharePoint on a SAN

Use SAN storage to get more magic out of SharePoint

by Todd O. Klindt

Technology is a funny thing. It can accomplish amazing, unimaginable feats—and then make you numb to them. I distinctly remember the first time I saw a demonstration of RAID 5. A colleague pulled a drive out of a running server . . . and it kept running! I was flabbergasted that it actually worked. Fortunately, being in the technology industry, I get to periodically experience these "Oh wow!" moments. It's part of why I love my job so much.

SANs are another example of technological magic. SANs allow us to pool storage in central locations, and then dole it out to individual servers, as needed. In this article, I cover how we can intelligently and responsibly use SANs in Microsoft SharePoint environments. Because SharePoint employs a complicated infrastructure, I also discuss how you can use SANs with supporting technologies such as Microsoft SQL Server and virtualization hosts. By the end of this article, you'll have a good understanding of how SANs work with SharePoint and its friends, as well as how best to use the technology in your production environments.

Some SAN Basics

At a basic, physical level, a SAN is a box the size of a refrigerator, filled with hard disks. (Blinking lights everywhere; it can be quite soothing sometimes.) These disks can be carved into an infinite number of combinations, using every RAID level we've ever heard of, and even a couple we haven't. These combinations (called logical unit numbers—LUNs) are presented to servers and appear as local storage.

This approach provides many benefits. It allows us to centralize storage, making it easier to get a snapshot of our storage usage and needs. It also gives us the flexibility of adding storage to our servers without doing the "RAID drive shuffle" each time we want to expand the storage. SANs also provide additional disaster recovery options. Most SANs support mirroring drives within the SAN, and many offer the ability to mirror the drives to another SAN enclosure.

In some cases, SAN storage can be faster than the DAS that might come with a server. SANs are highly tuned devices and routinely have many gigabytes of cache, which can result in very good performance.

A word of caution about performance is due here. To many of us, SANs are magic boxes that provide bountiful storage and unlimited performance. We assume they're configured correctly and that they will be fast. That isn't always a correct assumption.

Those shelves and shelves of hard disks in the SAN don't configure themselves. Someone needs to go in and decide how to best group those disks for the application for which they'll be used. File servers are happy enough with RAID 5; SQL Server transaction logs perform best with mirroring, or RAID 1. However, just because we're running a SQL Server doesn't mean that the LUN we're using for the transaction logs must be RAID 1. We might have different tiers of the same type of application.

For example, one SQL Server instance might have the databases for an application that requires speed, whereas another might store the databases for a rarely used legacy application and so can use slower, less-expensive storage. Knowing the type of load and the I/O performance that it requires is an important part of working with your storage team to make sure your needs are met.

To illustrate this point, imagine a SAN shelf with ten 300GB disks. These disks can be carved up and exposed in different ways, each having an effect on their performance. For instance, those ten disks can be configured as RAID 6, which means that two drives are used for parity, and the available storage is (n-2) × drive size (in our case, 8 × 300GB = 2.4TB). This 2.4TB of storage can be exposed as a single LUN or split into smaller LUNs. The server consuming that LUN or LUNs has no idea how it's configured on the back end. RAID 6 has good read performance but poor write performance because the parity bits must be calculated before the data can be written. That configuration is a bad fit for SQL Server transaction logs, which benefit from fast write times.

On the other end of the spectrum, those same ten 300GB drives could be configured as a RAID 1 mirror, providing 1.5TB of storage. This LUN would have much better write performance than the previous example, but it provides less storage. Same SAN, same disks—radically different experience for the server consuming those disks.

SharePoint on a SAN

When it comes to disk usage, SharePoint is a bit like a younger sibling. It doesn't use much I/O itself; it talks its siblings into doing all the heavy lifting (and taking all the blame). The Microsoft article "Capacity management and sizing overview for SharePoint Server 2010" (technet.microsoft.com/en-us/library/ff758647.aspx) doesn't even discuss the I/O that's needed for SharePoint Server 2010, only for SQL Server. This article assumes that any hard disks you can scrape together to host SharePoint will be more than sufficient for the program's modest demands. For the most part, this assumption is correct. If you have a SAN, though, you can leverage it to make SharePoint a little easier to manage and to tweak SharePoint's performance.

From a management standpoint, SANs make it easy to adjust the size and number of SharePoint's hard disks. According to the Microsoft article "Hardware and software requirements (SharePoint Server 2010)" (technet.microsoft.com/en-us/library/cc262485.aspx), SharePoint's only disk requirement is an 80GB system drive.

SharePoint itself doesn't need much disk space: It uses about 1GB, excluding logs, search index files, and any custom solutions. But that disk also needs to hold Windows and all its associated patches for the next few years. And the disk needs enough space for SharePoint's logs, plus enough space to perform a memory dump in the unlikely event of a problem. Also,

> SharePoint doesn't use much I/O itself; it talks its siblings into doing all the heavy lifting (and taking all the blame).

NTFS gets fussy when disks are more than 90-percent full, so leave enough space for some overhead, too.

SharePoint requires at least 80GB, but sometimes that isn't enough. If a SAN is hosting your SharePoint drives, expanding that 80GB system drive to, say, 120GB is painless. The SAN administrators turn a few knobs, pull a few levers, and Windows thinks it has a 120GB physical disk. A quick trip to Disk Manager, and your server now has 40GB more storage. Try that with a physical hard disk.

Performance is another area in which proper use of a SAN can help SharePoint. For the most part, SharePoint is understanding when it comes to performance, and its demands aren't very . . . well, demanding. SharePoint needs little to read from the local disk, and what it does need, it loads and caches. Still, disk performance can improve users' experience with SharePoint in a couple places: BLOB caching and search. Let's start by discussing BLOB caching.

BLOB Cache

In the context of SharePoint, BLOBs are files such as JPGs, GIFs, and MP3s. Large binary objects such as these don't change very often, so they're great candidates for caching. And because their size is usually large compared with the page size, they benefit the most from the process.

BLOB caching is a function of Microsoft IIS and is configured in each web application's web.config file (usually located in C:\inetpub\wwwroot\wss\virtualdirectories). Because wading through line after line of XML to make changes isn't for the faint of heart, SharePoint makes it easy for us to take advantage of BLOB caching. When SharePoint creates a web application, the program puts all the settings needed for BLOB caching in each web.config file—but doesn't turn on BLOB caching. How very thoughtful! To take advantage of BLOB caching, you need only find the relevant line in web.config and change the *enabled* value from false to true.

Figure 1 shows how the line looks before being altered. This figure is chockfull of good information, all of which Microsoft documents well. For this article, we're interested only in the *location* and *maxsize* parameters. By default, the location is set to the C drive. That makes some sense, because every Windows computer under the sun has that drive. However, it's a good practice to move as much as possible off the C drive, and BLOB caching is no exception. The BLOB cache location should be a secondary drive. That's where our SAN comes into play.

The reason we're turning on caching in the first place is to improve performance for end users. Each time IIS can serve up a file locally instead of pestering the back-end SQL Server instance, that file gets into the user's hands more quickly—which

```
<BlobCache location="C:\BlobCache\14"
  path="\.(gif|jpg|jpeg|jpe|jfif|bmp|
  dib|tif|tiff|ico|png|wdp|hdp|css|js
  |asf|avi|flv|m4v|mov|mp3|mp4|mpeg|mpg
  |rm|rmvb|wma|wmv)$" maxSize="10"
  enabled="false" />
```

Figure 1: Before enabling BLOB caching

makes for happy users. By putting the BLOB cache location on a SAN drive that's configured for high performance, we can get that file to end users as quickly as possible. The maxsize parameter dictates how large (in gigabytes) this web application's BLOB can be. The default is 10GB. The larger the cache, the more things can be cached and retrieved quickly. Remember that this setting is per web application, so make sure to plan for enough space. You'll also need to edit the web.config file for each web application on each server in your farm.

Search

SharePoint search can benefit the most from a high-performing SAN drive. Search has two primary roles: index and query. Both enjoy performance improvements from speedier I/O.

Index comes first. During indexing (and crawling, a related task), SharePoint scours itself and other configured content sources for the documents that you want to be discoverable in SharePoint. The files are crawled and then copied to the index server's RAM, where they're broken apart by an iFilter (not unlike a coconut on a rock), and all the words are listed. Those words are written to the index files on the index server's file system. The faster the index server can get those words out of its memory and onto its file system, the faster it can move on to the next file in its list. The larger your SharePoint farm gets, the more important crawl times are. A fast SAN drive on your index servers can reduce those times.

After your files have been indexed, they can be found by users. This is where the query servers come into play. As the index servers index files and write the information to their file system, that information is combined with the existing index files on the query servers. When a user searches for a document in SharePoint, the query servers spring into action. They take the user's search term and compare it to the index files on their file system, looking for matches. As your farm grows larger, the number of documents the query server must slog through grows as well. User queries take longer and longer. At some point, your users will become impatient as they wait for results. (And they'll spend that waiting time plotting ways to make sure that there's no Mountain Dew left in the cafeteria by the time you get there.) Putting the index files on a SAN drive with fast read performance reduces the time that's needed for queries to run. (Your users will be happy, and your tummy can get all the sweet caffeinated deliciousness it requires.)

As with the BLOB cache mentioned earlier, getting the index files off the C drive and onto a secondary drive is the best approach. If your query component is already configured to store its index files on the C drive, don't fret. The Search service deals well with change and happily lets you move the index to a different drive at a moment's notice. To do so, edit the Search Service Application Topology in Central Administration. For each of your index partitions, edit the value in the *Location of Index* field. Figure 2 shows an example in which the location has been changed to the D drive, which is hopefully a super-fast SAN drive.

I recommend just changing the drive letter; don't get crazy with the path. Leave the index files in their usual path. Doing so makes it easier when dealing with material that refers to the files in the default location, and it'll make it easier for someone else to step into your shoes after you get that big promotion or win the lottery. After you've changed the path, click OK and then click Apply Topology Changes.

Search is happy to move your index files for you, but it's in no rush to do so. The service's first concern is being able to respond to end-user requests, so moving the index doesn't get its full attention. Depending on the size of your index, the move process could take a while. It's worth the wait, though. After your index files are on a blazing fast SAN drive, your users will no longer be plotting your demise.

Virtualization on a SAN

SharePoint relies pretty heavily on other technologies to render pages for your users. In some cases, those technologies can make use of a SAN. Virtualization is one example. These days, almost every SharePoint farm has at least one virtualized server. In many cases, the entire farm (test or production) is virtualized. Whether you use virtualization software from Microsoft, VMware, or Jim-Bob's Discount Virtualization, it all can benefit from speedy SAN drives—or suffer from poor decisions.

All major virtualization software suites support hosting guests on SAN drives. You should consider the purpose of a farm (i.e., development, test, or production) when deciding how to configure the SAN drives that host that farm. Development farms, for instance, can have all their drives carved from the same spindles because their performance isn't important. If the servers in the farm are slow, only the developers are affected, and honestly, I'm OK with that. (It teaches them patience.) Test farms might need a little better performance, so those servers should be hosted on better-performing SAN drives. Production farms, if they're virtualized and using SAN drives, should have the

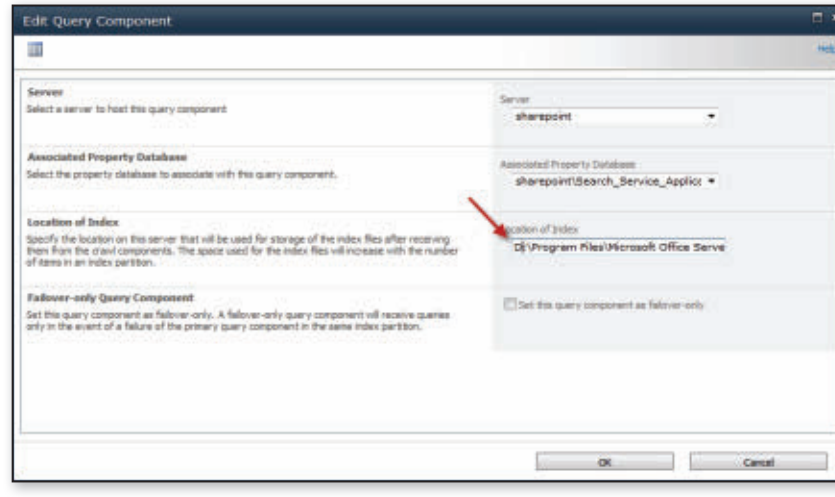


Figure 2: Moving the index files

best-performing LUNs that the SAN can provide. Unfortunately, there's no good way for you, as the SharePoint administrator, to know how your LUNs are configured. You'll need to take your storage administrators' word for it. Don't be afraid to bribe them with gifts of candy and World of Warcraft figurines.

SQL Server on a SAN

If I've said it once, I've said it 100 times: "SharePoint gets all its performance from SQL Server." In the beginning of this article, I talked about how different SAN configurations affect performance. Nowhere is that more important than with SQL Server. Every document, every list item, every search result, and every user profile is delivered out of a SQL Server database. If those databases are on a slow drive, then SQL Server is slow. If SQL Server is slow, then no amount of configuration trickery or swearing can make SharePoint fast. SQL Server really is that important.

The Microsoft article "Storage and SQL Server capacity planning and configuration (SharePoint Server 2010)" at technet.microsoft.com/en-us/library/cc298801.aspx gives some guidance on which services rely heavily on SQL Server I/O and how to calculate the I/O operations per second (IOPS) that you'll need for SharePoint. Again, there's no way to determine the configuration of the SAN drives that SQL Server is using. You can, however, use a tool such as the Microsoft SQLIO disk subsystem benchmark tool to determine the IOPS of the drives in the system. You can use this information to determine whether the drives are up to the task of supporting SharePoint. If they aren't, then you can work with your storage team to get the performance you need. (Although this article is about SAN drives, SQLIO works just as well with physical disks if you're curious to see how they're performing as well.) To download the tool, go to www.microsoft.com/download/en/details.aspx?&id=20163.

The Magic of SAN

Any SharePoint administrator worth his or her salt knows that SharePoint is a complicated beast. It has its fingers in Windows, IIS, and SQL Server, to name a few places. Many of these aspects of SharePoint can benefit from the magic of a SAN. SharePoint can use a SAN to cache frequently used files or store search index files. SharePoint servers can be virtualized on SAN drives, and SharePoint can use SQL Server databases that are stored on SAN drives. Regardless of how you leverage SANs for your SharePoint environment, keep your eyes on performance, and make sure to watch those blinking lights at least once. They're mesmerizing.

InstantDoc ID 141962

Todd O. Klindt
(todd@sharepoint911.com) is a consultant for SharePoint911 and a SharePoint MVP.

- Automation Anywhere
- Symantec
- CENTREL Solutions
- Azaleos

Free SurDoc Platform Features Document Signing and 10GB of Cloud Storage Space

SurDoc introduced its secure document-signing feature on its SurDoc platform. The capability is the first of its kind in the industry to be integrated into a cloud storage environment. Traditionally, mobile workers who regularly execute forms and contracts must download documents, and then print, sign, scan, upload, and email these documents to be able to perform their jobs. With SurDoc, these workers now have an easy, fast, secure, and reliable option to access, edit, sign, and send forms and contracts from any location digitally. SurDoc currently offers 10GB of space, the largest amount of free cloud storage available for individual users. In addition to the secure document-signing functionality, the free platform includes a typewriter tool and a handwriting tool, which functions like a pen for signing and dating documents. For more information, contact SurDoc at www.surdoc.com.

XIA Configuration Server 2012 Standardizes and Automates Documentation

CENTREL Solutions' XIA Configuration Server 2012 automates and standardizes technical documentation for your IT infrastructure, closing the loop on knowledge gaps within your organization. IT departments are provided access to detailed technical information that is normally difficult or impossible to acquire at critical times. This is beneficial when performing changes to the environment and during disaster recovery situations. The automated nature of the product saves countless hours required to manually document network configuration and allows for automated version control. This means users can track changes to the environment and easily spot unauthorized configuration changes. XIA Configuration strives to give you a single location where IT support providers, decision makers, and customers can access all of their technical information in a standardized format. For more information, see centrel-solutions.com/xiaconfiguration.

PRODUCT SPOTLIGHT

Automation Anywhere Achieves Microsoft Gold ISV Competency

Automation Anywhere announced that it achieved a Gold Independent Software Vendor (ISV) Competency in the Microsoft Partner Network. To earn a Microsoft Gold Competency, organizations must complete a rigorous set of tests to prove a certain level of technology expertise, have the right number of Microsoft Certified Professionals, submit customer references, and demonstrate a commitment to customer satisfaction by participating in an annual survey.

"We are absolutely delighted to announce this achievement," said Mihir Shukla, Automation Anywhere CEO. "A Gold ISV Competency differentiates us from the competition and establishes us as a market leader, further demonstrating our commitment to serving the needs of customers relying on Microsoft-based solutions. Combining our automation solution with the power of products like Microsoft Windows, Microsoft Office, and Microsoft Dynamics brings more value to the customer. The ability of Automation Anywhere 7.0 Enterprise to leverage the business potential of solutions from Microsoft further helps our customers and makes their business processes more productive, secure, and efficient."

As a result of this partnership, Automation Anywhere 7.0 Enterprise now provides customers with a complete solution for moving data to and from Office applications such as Excel and Access. The solution provides complete, centralized control over all automation processes, enables management of hundreds of users, and allows hundreds of processes to be scheduled and launched at once. For more information about Automation Anywhere, please visit www.automationanywhere.com.

Guidance Software Expands EnCase eDiscovery Cloud Support

Guidance Software announced a new version of its EnCase eDiscovery software with the ability to collect electronically stored information from more cloud-based data services and a new collected data re-use feature for searching evidence collected for previous cases. The new capabilities are available in EnCase eDiscovery 4.4 and help corporate IT and legal teams to confidently assert that they have searched all of the potentially relevant electronically stored information in their possession, custody, or control. The Collected Data Re-use (CDR) feature allows e-discovery teams to search already collected evidence residing in an EnCase

Logical Evidence File (LEF) from a previous matter. This reduces legal risk, cuts e-discovery collection time, and reduces the impact on custodians. For more information, visit www.guidancesoftware.com.

Symantec Releases Backup Exec 2012 and NetBackup 7.5

Symantec announced the release of Backup Exec 2012 and NetBackup 7.5, both of which provide options that let you tailor the solution to your unique needs—whether you manage a small-to-midsized business (SMB) or an enterprise. Symantec has also made backup more effective for partners to help their customers protect critical business information without breaking the budget or feeling the pains from the difficulty and intricacy that is often associated with backup. Essentially, Symantec recognizes the need to simplify, automate, and modernize backup—particularly in light of recent survey results the company collected: Only 28 percent of respondents were completely confident that 100 percent of the backed-up data could be recovered; 72 percent stated they would switch backup products if backup speeds doubled; only 58 percent of respondents believed their virtualization backup was adequately/perfectly working; and 28 percent said they have too many backup tools. To see how Symantec tackles these problems with its upgraded solutions, go to www.symantec.com.

Azaleos Expands Reach of Managed SharePoint Private Cloud Services

Azaleos announced two new services designed for enterprises that want a new Microsoft SharePoint 2010 system that deploys quickly and doesn't require local IT management. Azaleos SharePoint Starter Edition and Azaleos SharePoint Core Edition provide drop-and-go managed SharePoint outsourcing alternatives to the existing Azaleos SharePoint Premier Edition. Azaleos SharePoint Starter Edition enables smaller enterprises and departments within large enterprises to get a simple managed SharePoint system up and running quickly. For larger enterprises adopting the powerful collaboration system for the first time, but uncertain of their needs, SharePoint Core Edition provides more robust management services with a fixed set of functionality. For more information about these two new services, visit www.azaleos.com

ConferenceEdge's New API Platform Connects Businesses to Event Automation and Logistics

ConferenceEdge launched its enhanced event APIs for integration with both public and proprietary systems. These APIs will allow businesses to easily take advantage of the powerful logistical features from within the platform while still maintaining the integrity of their existing workflows. Both enterprises and SMBs can easily take advantage of powerful automation utilizing event APIs for virtual and physical events. ConferenceEdge event APIs were developed to provide a better alternative to the traditional event registration and management processes that require you to work solely within certain business rules and workflows. For more information, contact ConferenceEdge at www.conferenceedge.com.

Paul's Picks

www.winsupersite.com

SUMMARIES of in-depth product reviews on Paul Thurrott's SuperSite for Windows

Microsoft Hotmail

PROS: Great web UI; excellent performance; integrates with other Microsoft products

CONS: Lacks two-factor authentication

RATING: ◆◆◆◆◇

RECOMMENDATION: For cloud-based email, contacts, and calendar services, Microsoft has two big offerings: Hotmail and Office 365. Hotmail offers an efficient web interface, works with Windows Live Mail and Outlook on the PC desktop, and is compatible with virtually any mobile device. It lacks two-factor authentication (see Gmail). And for aggregated email accounts, messages sent as if from another account bear an "On Behalf Of" header, making some spam filters skittish. I give it the nod. It's what I use.

CONTACT: Microsoft • www.microsoft.com

DISCUSSION: www.winsupersite.com/article/windows-live/hotmail-exchange-email-141856 and www.winsupersite.com/article/windows-live/gmail-hotmail-update-142061

Microsoft Office 365 for Individuals and Small Businesses

PROS: Exchange-based email, contacts, and calendar; SharePoint Online collaboration

CONS: Lync Online lacks many on-premises features; configuration can be difficult

RATING: ◆◆◆◆◇

RECOMMENDATION: Office 365's Plan P, for small businesses and IT pros (i.e., individuals), offers the right price: $6 per user per month. If you can get past the hurdle of configuring it—hint: employ a Microsoft partner—Office 365 is pretty incredible, with Exchange Online–based email, calendar, contacts, and tasks management; SharePoint Online–based document collaboration; a private version of the Office Web Apps; and a limited version of Lync Online. Adding Office 2010 Professional Plus costs an additional $15 per user per month. I'd like to see less expensive options and simpler configuration, but it's still great, especially for SMBs.

CONTACT: Microsoft • www.microsoft.com

DISCUSSION: www.winsupersite.com/article/office-365/office-365-individuals-small-businesses-141934

InstantDoc ID 142239

AirMagnet WiFi Analyzer PRO

With the purchase of AirMagnet in 2009, Fluke Networks expanded its portfolio of network-monitoring tools. Today, these network products are still sold under the AirMagnet brand. One of these products, WiFi Analyzer PRO, is focused on auditing, monitoring, and troubleshooting wireless LAN (WLAN) networks.

Fluke Networks provided me with an unrestricted trial license, so I tested the full version of WiFi Analyzer PRO. The company also provided me with four 802.11n USB wireless adapters produced by Proxim Wireless: one to use as a standalone adapter and three to use with a USB hub to test the product's Roaming Analyzer feature. Not all USB wireless adapters will work with the product, so Fluke Networks provides a list of tested and approved adapters. The list includes adapters that fully support all the product's features and adapters that support only some features. The Proxim Wireless adapters I was provided are 100 percent certified to work with the product.

I tested the product on a laptop running Windows 7 SP1 64-bit. Downloading and installing the product was simple. I was very pleased to see that the installer didn't spray icons on my desktop or otherwise do anything to make a pest of itself. The only hang-up I encountered was installing the drivers for the USB wireless adapters. The drivers are included with the installation package but aren't installed automatically. A separate setup program has to be launched to install the drivers. I would've liked the product's installation routine to ask if I was going to use the Proxim Wireless adapters and install the drivers for me.

Upon starting the application, I was greeted with a colorful dashboard that immediately began to populate with information about the wireless networks that were around me. I was impressed that, in addition to the usual suspects—such as signal strength reported in decibels—the application also reported such details as the most utilized wireless channels, the most "chatty" wireless stations, and the number of devices in each Wi-Fi standard (a, b, g, and n) broken down into access points (APs), ordinary stations (e.g., laptops), and stations acting in ad-hoc mode. Just by glancing at the default dashboard, it would be easy to make a snap decision about which channel to use if I were installing a new AP, for example.

Fortunately, the product doesn't stop there. Another impressive ability of the application is how easy it is to drill down to find exactly the information needed. By clicking on the AP tab, for example, I was presented with a list of all the APs within range of the Proxim Wireless adapter. The sensitivity was excellent, finding APs well beyond the range of my laptop's built-in wireless card. One icon appearing on the left side of some of the listed APs was a red alarm bell. Here is where one of the greatest strengths of the product comes though: WLAN auditing.

By simply clicking that red alarm icon, I was presented with a list of potential problems involving the AP in question. I saw some problems I was expecting, such as utilizing Wired Equivalent Privacy (WEP) instead of the far more secure Wi-Fi Protected Access (WPA). However, the application also highlighted a problem I didn't expect to see: The AP was reporting an available speed that didn't match the configured wireless band. The software suggested that the AP might be configured incorrectly, and upon examining the AP, I found that it was!

I wasn't able to fully explore the Roaming Analyzer feature because of the suburban location where I was conducting my testing. This location consisted of only a dozen or so independent WLANs with little or no roaming between APs. However, I did manage to test the three-USB-wireless-adapter configuration that would be utilized for this feature and came away very impressed. Just by utilizing the additional wireless adapters, the scanning speed of the application improved dramatically. The dashboard widgets updated extremely quickly, and it was really neat to see an instantaneous view of the airwaves updating in near real-time, with the ability to drill down into a certain area to obtain further details.

WiFi Analyzer PRO includes detailed reporting options, including precanned reports available to help IT pros meet compliance-reporting requirements, such as those for the Sarbanes-Oxley (SOX) Act and Payment Card Industry Data Security Standards (PCI DSS). It also includes tools for not only troubleshooting performance problems but also simulating potential performance effects if you were to add more APs or stations.

Having used numerous network analysis tools in the past, I came away quite impressed with WiFi Analyzer PRO. Although there are many excellent free utilities on the market for performing wireless network analysis, this product goes above and beyond them to provide full visibility into the plethora of wireless networks that surround us all. If you work with Wi-Fi networks regularly and need an all-in-one analysis tool, this product is recommended for sure.

InstantDoc ID 142219

AirMagnet WiFi Analyzer PRO

PROS: Deep visibility into all aspects of wireless networking, including security and performance recommendations, packet analysis, and integrated reporting

CONS: Drivers for wireless adapters not automatically installed; expensive if used infrequently

RATING: ◆◆◆◆◆

PRICE: $3,995 for AirMagnet WiFi Analyzer PRO, $495 for multi-adapter kit (pricing might vary depending on country and region, so check with local sales representative)

RECOMMENDATION: If your work includes constant analysis and troubleshooting of wireless networks, this product should be on your short list of tools to consider adding to your arsenal.

CONTACT: Fluke Networks • 800-283-5853 or 408-753-1500 • www.flukenetworks.com

Michael Dragone | articles@mikerochip.com

REVIEW

Symantec NetBackup 5220

As amazing as it sounds, many companies still don't pay adequate attention to their backup strategy and run the risk of losing crucial data due to server failure or user error. Some companies might find out too late that the data stored in their databases, document collaboration systems, or email systems didn't get backed up because their backup solution was out of date, unable to work with modern applications, or meant to handle only file-level backups.

There are many available backup solutions that companies can buy and install on their own servers. However, there are far fewer backup appliances. One noteworthy offering is the Symantec NetBackup 5200, which runs the same NetBackup software that companies can buy and install on their own hardware. The basic NetBackup 5220 appliance comes with two 1GB network ports: one for initial configuration using a laptop computer and the other for connecting the appliance to the network. The device has slots for additional network ports. The basic unit ships with 4TB of disk space but can be expanded.

I recently installed, configured, and used a NetBackup 5220 appliance. I was impressed by the rich feature set and performance offered. However, I did encounter a few problems.

The Initial Configuration

You begin by connecting your laptop to the configuration network port using a crossover network cable, opening your browser, and connecting to 192.168.1.1. This is where I first encountered a problem, as that address was being used by my primary firewall on my network. To fix the problem, I had to change the configuration port's IP address to one outside of any subnet range I was using, which can only be done from the command line. Symantec confirmed that this was a known issue and said that a future version of the *Getting Started* guide would address the problem and provide a workaround.

Next, you provide configuration information. In addition to specifying the network parameters (e.g., IP addresses for all NICs), you specify a password for the built-in administrator account, Network Time Protocol (NTP) information, and whether to use DNS or a local HOSTS file for client name and address resolution. You also specify whether the appliance will take the role of a Master or Media server. In a new deployment, the first appliance will be a Master server. Additional servers typically are Media servers, which let you expand the amount of disk space available for backups. However, you can install multiple Master servers in a deployment.

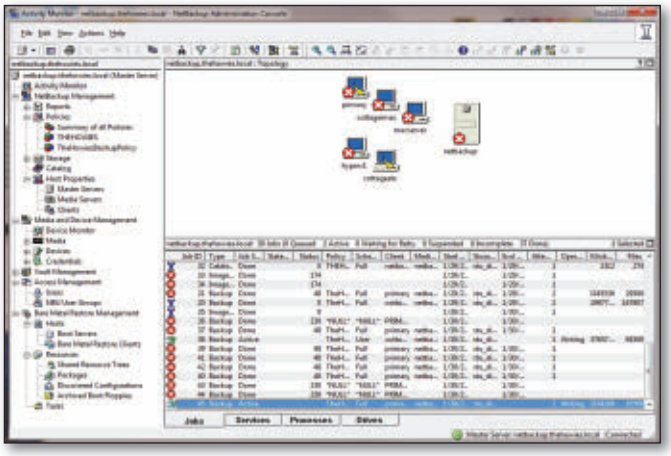


Figure 1: The management console

When you configure an appliance as a Master server, you can configure the internal storage into either Deduplication storage (the default) or AdvancedDisk storage. Unless you have a specific need, I recommend you use the default option.

After you've entered the configuration information, the appliance performs the initial configuration and prepares the internal storage. This can take quite some time. During testing, my laptop went to sleep due to inactivity while the device was being configured. This caused the initial configuration to fail, and I had to start over after turning off the power-saving functionality on my laptop.

Once the initial configuration is complete, you can use a web browser to connect to the appliance using your network's IP address. Note that not all browsers are supported. Your web browser needs to run Microsoft Internet Explorer (IE) 7.0 or later or Firefox 3.0 or later. Also note that you'll run into problems when connecting to the appliance if IE is configured to use enhanced security.

The Management Console

The next step is to install and configure the management console on a management workstation. The installation software for the management console is hosted on the appliance's home web page. There are versions for a variety of OSs, including Windows (32-bit and 64-bit versions of Windows XP and later), Mac OS, and HP-UX. On Windows, you must download and extract the management console installation package from a .zip file. The installation must be performed by a member of the local group Administrators. In addition, by default, any member of the local group Administrators will be able to manage the appliance using the management console. For these reasons, make sure that your management workstation is physically secured, uses a static IP address, and doesn't rely on DHCP for address assignment. When installing the management console, you'll be prompted to enter a license key—a prompt that you can ignore. Simply select Remote Administration as the installation mode. Both the management console and the backup software will then be installed on the computer.

John Howie | jhowie@microsoft.com

After I installed the management console, I wasn't able to get it to connect to the Master server appliance. I found out that there is another step, which isn't documented anywhere. You have to use a browser to connect to the appliance and add the name of the management workstation to the appliance as a server on the Appliance tab of the Manage page.

As Figure 1 shows, the management console appears as a dense, confusing tool with a wide variety of options to the uninitiated. It isn't well laid out and will likely seem daunting to any user who doesn't use it frequently.

The NetBackup Software

Before any system can be backed up, the NetBackup software on the appliance must be configured. The first time you launch the management console, a wizard walks you through a set of tasks to manage storage, create catalogs, and configure backup and restore policies.

Backups are done by policy, not per backup client, so you must assign clients to backup policies before they can be backed up. A client can be in one or more backup policies, so if a server with multiple applications is a backup client, you can back it up several ways to ensure that no data is missed. It's during this configuration process that you start to see the power and flexibility of the NetBackup software. For example, you can configure policies that allow end users to perform their own backup and restore operations. In addition, multiple client OSs are supported.

Any client you want to back up must have the NetBackup client software installed on it. On Windows systems, the easiest and most reliable way to install the software is to map the share \\<appliancename>\install to a drive letter and run quickinstall.exe. For UNIX and other types of client OSs, you can mount the share using NFS and run an installer that detects what variant of UNIX or Linux they're running and installs the appropriate client software.

Backing Up and Restoring Clients

Backup administrators can use the management console to schedule backups or perform one-time backups. Although backups are done by policy (and not per client), you can select one or more clients in a policy and back up just those.

The client software includes a client application. Despite being an old-style multiple-document interface (MDI) application, the Windows client application is powerful. It lets you manage different backup and restore operations simultaneously. You can even prepare a backup client for a bare-metal restore if you have to rebuild it from scratch. End users can also use the client application to back up their drives, folders, files, machine state, and even data stored in applications such as email systems (assuming they have the permissions to do so). Before a client can be backed up, it must be assigned to one or more backup policies on the appliance.

During testing, I ran into another problem. The Linux OS that the NetBackup appliance uses supports Multicast DNS, so every lookup of a Fully Qualified Domain Name (FQDN) that ended in .local failed. Only after searching the Symantec support site did I find a solution. The solution requires that you use the Linux command line on the appliance to turn off Multicast DNS or instead use the local /etc/hosts file on the appliance for name and address resolution. However, the latter approach could become unwieldy in environments with hundreds of servers. Plus, you must use the web interface or command line on the appliance to add entries to the local /etc/hosts file. I spoke with a Symantec representative about this, and he recognized it was an issue and said steps would be taken to correct it, even though it's not a problem with the NetBackup software itself.

Restoring files is a breeze for end users and administrators. Using the client software, end users can simply select the desired backup file from the set of available backups and select the folders and files to restore. I found the restore operation to be extremely fast. Administrators can restore files to their original location, a different location, or even a Virtual Hard Disk (VHD). This last option is extremely powerful, as you can then mount the VHD onto a virtual machine (VM).

Virtualization Support

The NetBackup 5220 appliance supports virtualization, which is where NetBackup truly shines. You can back up VMs on Microsoft Hyper-V and VMware vSphere Hypervisor (formerly VMware ESXi) hosts without the need to install the NetBackup client software on the VMs, as long as the software is installed on the host.

NetBackup uses the Volume Shadow Copy Service (VSS) on Hyper-V hosts and vStorage on VMware hosts. This means that the virtual disks associated with the VMs must be on storage disks attached to the server. If you use iSCSI or physical disks for VMs' hard drives, you'll need to install the NetBackup client software on the VMs.

A Great Appliance Overall

NetBackup 5220 is a terrific appliance primarily designed for enterprise data center use. However, it's also well suited for remote offices and as a supplement to existing NetBackup solutions that require additional backup capacity. Organizations that use virtualization heavily might also want to look at the NetBackup 5220 appliance as a solution to their backup requirements.

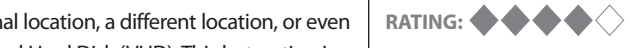
I believe that the problems I ran into installing, configuring, and using the appliance are edge cases that you'd expect a support team to have to deal with. I would certainly encourage large and midsized enterprises to seriously consider the NetBackup appliance if they need to build a backup infrastructure or supplement an existing one.

InstantDoc ID 142192

Symantec NetBackup 5220

PROS: All the power and flexibility of NetBackup software in an appliance; expandable to 36TB of disk and can be integrated into existing NetBackup systems; support for many different types of OSs and server-side applications (e.g., databases); great virtualization support

CONS: Configuration can be problematic in some environments; management interface is confusing and difficult to work with unless you use it regularly; documentation isn't great

RATING: 

PRICE: Starts at $23,795

RECOMMENDATION: Symantec NetBackup 5220 is ideal for large enterprises' data centers and remote offices but might also be of interest to midsized enterprises with sophisticated backup needs and organizations that are heavy users of virtualization.

CONTACT: Symantec • 650-527-8000 • www.symantec.com

Hybrid Solid State Disk Solutions

High performance and capacity at a lower cost than pure SSDs

by Michael Dragone

Solid state disks (SSDs) are a popular replacement for standard magnetic hard disk drives. I've used several SSDs in my various computers over the past few years and can vouch for the extreme performance increase, not to mention the reduced heat and noise and excellent power savings. The only drawback is the price of such devices. For use as local storage, the price of SSDs has come down greatly over the past few years while the raw capacity of magnetic drives has gone up. This leads to a difficult decision between a slower but larger-capacity magnetic drive and a faster but smaller-capacity SSD. In many cases, the extra capacity of magnetic drives is hard to ignore, despite the extreme speeds that are possible only with SSDs.

SSDs quickly moved from being used only in local storage to being used in network storage. Products such as Texas Memory Systems' RamSan offer great performance in a small package, but, again, the main drawback is price. Many IT pros are left asking themselves if the price-performance trade-off is worth it. After all, not every workload needs the performance that SSDs provide. For example, it makes more sense to store archived files that are accessed rarely or not at all on less expensive hard disk drives than SSDs. But what if you need the speed that SSDs provide but only at certain times of the year (e.g., during tax season)? Or what if you have an application or set of applications that needs the best performance possible, but the cost of an SSD solution is out of your budget?

Fortunately, many vendors jumped on the bandwagon of combining SSDs and hard disk drives, including:

- Dell EqualLogic (www.equallogic.com)
- Fujitsu (solutions.us.fujitsu.com)
- NetApp (www.netapp.com)
- NexGen Storage (www.nexgenstorage.com)
- XIO Storage (www.xiostorage.com)

These vendors' hybrid SSD solutions endeavor to balance the best of both worlds: the lower price and larger capacity of hard disk drives with the higher performance and reliability offered by SSDs.

As with everything else in IT, however, nothing is that simple. After speaking with several vendors and doing some research, I learned that not every hybrid SSD solution is created equal. These products are really all about the software that controls them. In this article, I'll focus on two vendors—XIO Storage and NexGen Storage—that focus on providing the best possible performance through their customized software yet differ in how they physically build their hybrid SSD solutions.

XIO Storage

"We do things definitely different, but our lineage goes back for years," Steve Sicola, CTO of XIO Storage told me when I spoke to him about Hyper ISE, the company's hybrid SSD solution. Hyper ISE is a storage array that combines multiple "data packs" consisting of 10 hard disk drives and 10 SSDs in one sealed unit. Data is moved between the adaptive DRAM cache, the hard disk drives, and the SSDs.

Keith Hageman, storage technology evangelist at XIO Storage, expanded on the solution a bit more. "The hottest data gets moved to the SSDs. Cooler data remains on the hard drives. From the server and OS standpoint, it looks like the same LUN."

Hyper ISE takes care of the movement of the data automatically. Every five seconds, the Hyper ISE software checks to see whether the "hottest" 120MB block of data is present on the SSDs. If it isn't, the software moves the hottest data from the hard disk drives to the SSDs.

"We write [the data] to the adaptive DRAM cache first, then the hard drives, and then move it to the SSDs," Sicola said. Because all the data is written to the hard disk drives first, there's a bit of a performance hit when the array is first installed. "By taking the initial writes of the data to the hard drives, we don't have the best performance at startup," Hageman explained. Over time, however, the software moves the 120MB block of hot data to the SSDs, where the best performance exists. Furthermore, the Hyper ISE software is intelligent. It has been "taught" what various workloads (e.g., Microsoft SQL Server workloads, Microsoft Exchange Server workloads) "look like" so that when a data stream comes into the array, the software knows how to best optimize the data placement on disk.

"We've been actively working with the Microsoft SQL Server 2012 team," Hageman told me. "In 2010, the best [SQL Server] performance was on a Hitachi solution, utilizing almost 500 15,000rpm hard disk drives across multiple racks. They delivered 5,400 transactions per second on a 7TB data set at a cost of over $2 million. In 2011, our product handled 11,500 transactions per second in only 3U of rack space with 40 drives at a cost of only $150,000."

NexGen Storage

Although most of the vendors that incorporate SSDs into their solutions are well-known and established in the storage industry (e.g., Dell EqualLogic, NetApp, Fujitsu), there are some fresh new "faces," such as NexGen Storage. When I spoke with Chris McCall, vice president of marketing for NexGen Storage, he mentioned that NexGen and its n5 Storage System "just came out of stealth mode" in November 2011.

"Our two founders came from Left-Hand Networks," McCall explained. "They have lots of knowledge about storage, iSCSI, and so on, and we wanted to take a fresh look at storage system architecture. The question we heard from customers was always: How many applications can I put on your SAN? Can I add 10 more applications? What will it do to the performance? It was a constant battle of trying to help the customer."

The answers to these questions are especially important in smaller organizations that need the higher performance that a hybrid SSD storage solution offers but don't have a dedicated team of storage experts who focus just on the storage solution. Many IT professionals in the small-to-midsized business (SMB) sector wear several hats. The n5 Storage System attempts to alleviate some of this management overhead.

"Just tell us how fast you want to go and the system will automatically tier it," said McCall. The NexGen product works off of a Quality of Service (QoS) number set by the administrator in terms of I/O operations per second (IOPS). If, for example, you know that the LUN dedicated to your SQL Server database files needs 20,000 IOPS, you set the NexGen product to provide that. The QoS settings are guaranteed minimums. So, for example, if you need 10,000 IOPS for a file server but the array has 20,000 IOPS available, the n5 Storage System would allow the file server to take advantage of the available 20,000 IOPS.

Another interesting aspect of NexGen's QoS approach is the ability to adjust the QoS on a schedule. For example, you can schedule a higher QoS for a two-hour window when a large report needs to be run. The n5 Storage System also optimizes performance based on the application using it. In other words, it "knows" what SQL Server data access looks like versus Exchange data access and adjusts the QoS accordingly.

Unlike Hyper ISE, the n5 Storage System writes to the SSD first and then moves data to the hard disk drives. The n5 Storage System utilizes up to four Fusion-io SSDs connected directly to the PCIe bus across a maximum of two active-active controllers. A 3U, 32TB n5 Storage System starts at $88,000. The n5 Storage System utilizes 7,200rpm Serial Attached SCSI (SAS) hard disk drives. The system supports up to three additional disk shelves if needed.

Conversely, the Hyper ISE utilizes 10,000rpm hard disk drives that are fixed within the data pack and aren't user accessible. Only the data pack itself is able to be removed and only if the system is powered off. I asked the XIO team how an administrator could replace a drive that failed.

"We have multiple patented processes to repair a drive in place," Sicola explained. "We have access to the drive manufacturing code directly from our drive vendor." Hageman continued: "If a drive really does get in trouble, we can re-manufacture the drive in the data pack."

Like Hyper ISE, the n5 Storage System offers additional features. For example, both products offer:

- Detailed reporting that shows how an application workload would behave if put on the hybrid SSD solution without actually doing so
- Management and monitoring software to ensure that the hybrid SSD solution is performing optimally

Different Approaches, Same Goal

Despite having different approaches, both XIO Storage and NexGen Storage are focused on the same goal: maximizing application performance automatically. And both vendors specifically told me that their software is what enables them to achieve this goal.

So, if you're in the market for a hybrid SSD storage solution, it's important to look past the raw numbers that storage vendors will put in front of you. Looking beyond the numbers to the intelligence that the vendors have built in to their products through their software could mean the difference between a storage solution that's highly optimized for your particular workloads and one that is just faster than the solution it replaced.

Although the cost of hybrid SSD solutions is still high, the price has come down considerably over the past few years. They're now at a price point that's attractive to even SMBs that need the most bang for their buck. Prices start well under $200,000, and performance is up to 10 times that of traditional magnetic drive arrays, so I encourage you to take a hard look at hybrid SSD storage solutions for your next project.

InstantDoc ID 142189

Michael Dragone (articles@mikerochip.com) is a contributing editor for *Windows IT Pro* and a senior network engineer. He holds MCDST, MCSE: Messaging, MCTS, and MCITP credentials and remembers when *Windows IT Pro* was called *Windows NT Magazine*.

Identity as a Service

IDaaS is moving from radical to mainstream

by Sean Deuby

Identity as a Service (IDaaS) was developed to deal with a new need that's arisen with the popularity of cloud computing: identity management for the exploding number of Software as a Service (SaaS) applications available on an almost instant basis. At the end of 2011, Gartner estimated that global SaaS revenue hit $12 billion, a 21 percent increase over 2010, and that SaaS will account for 15 percent of enterprise application purchases by 2015. And right along with this growth is the problem of how to manage user identities for all of these applications.

Adding the on-premises capability of securely managing cloud identities for SaaS applications requires some work. You need to set up an Internet single sign-on (SSO) federation solution, and once you've set it up, you have to manage it. One of the larger tasks in running your own federation solution is managing the relationships of the ever-increasing number of SaaS vendors. Many companies simply don't want to be adding these on-premises costs at the same time they're shifting some of their IT capabilities to the cloud.

IDaaS moves this heavy lifting from your premises to the cloud. Instead of running your own cloud identity management system, the IDaaS vendor does all the work. The IDaaS vendor sets up and maintains federated trusts for SaaS vendors that support federation, creates customized connections (such as forms-based authentication) for vendors that don't support it, manages account provisioning and deprovisioning, performs auditing, and provides a variety of other identity-related services. All the customer needs to do is set up an interface with the IDaaS vendor, which, depending on the complexity of the installation, can take as little as a few hours or as long as a month.

The leaders in the IDaaS market include Intel, Okta, OneLogin, PasswordBank Technologies, Ping Identity, and Symplified. Which IDaaS provider you choose depends on your requirements. Some providers, like Okta, focus on providing SSO to SaaS applications for an enterprise with an on-premises Active Directory (AD) system. Others provide a variety of possible configurations. For example, PasswordBank has seven IDaaS-related options and Symplified has a broad feature portfolio.

The IDaaS Technology

Security issues associated with SaaS applications have been gaining wider attention over the past six months, fueling business decision makers' interest in IDaaS. They're becoming increasingly aware that the IDaaS technology can solve their SaaS application security problems on a subscription basis. This top-down interest has been driving much of the adoption of IDaaS, despite IT's misgivings.

Before IT pros and their managers can accept how IDaaS solves some of the challenges associated with cloud identity, they must know what the challenges are. And before IT pros can understand the challenges, they must understand basic cloud identity technology.

IDaaS solutions contain two key components: the identity store and the identity portal. (For information about some of the other components, see "Outsourcing Your Identity with IDaaS," August 2011, InstantDoc ID 139563.) Each IDaaS solution has an identity store, which can be configured in a number of ways. Typically, this store contains a synchronized set of identities from an AD security group or organizational unit (OU) that is authorized to use the IDaaS service. These identities are then provisioned out to the cloud applications.

However, the identity store doesn't have to contain only identity data replicated from an enterprise. Using IDaaS as a hosted identity provider, a large company could keep its contractor identities in the cloud identity store, thus allowing access to a variety of applications while keeping the identities out of the corporate AD system.

The core UI component is the identity portal, where users log on once and are then provided access to the cloud services for which they've been authorized. This identity portal can be in the cloud, on an on-premises component, or in a browser add-on. For example, Symplified offers Identity Router,

which acts as an identity portal and proxy server. Through policies, it determines the identity store that users authenticate against. (It can be an on-premises identity store, a cloud identity provider such as Google, or Symplified's own identity store.) Identity Router then performs the authentication on behalf of the user, in whatever format the identity store requires. Identity Router can be installed as an on-premises managed hardware appliance or virtual machine (VM), or a VM in the cloud.

IDaaS Benefits

The popularity of IDaaS as a viable alternative to on-premises solutions is understandable, since it has a number of advantages over traditional solutions. The fact that Intel has entered the market is, to me, a validation of its potential growth. One advantage of IDaaS is that auditing SaaS application usage is often simpler than other solutions because all traffic accessing the cloud services goes either though an on-premises agent or directly through the IDaaS service portal. Okta, for example, provides audit information on user activation, user activity, user access, application usage, user provisioning, and user deprovisioning.

With on-premises federation solutions, it takes time to work out and establish trust relationships with the SaaS vendors that users need. With IDaaS, users can immediately get SSO access to thousands of SaaS applications (once they've subscribed to them). And the sooner you can get users to securely access these applications the better because they're likely already accessing these applications in an unsecure manner.

Some IDaaS providers offer aggregation services to make it easier to view on-premises identity data, which might be in many places, as a single instance to cloud applications. Symplified, for example, has a virtual directory service built into its product. Even if you haven't gotten your own internal identity management organized quite yet, a virtual directory service will take identity data from AD, relational databases, and miscellaneous LDAP directories, and create a consolidated view for SaaS applications to consume. (For more information about virtual directory services, see "The Rise of Virtual Directory Servers," InstantDoc ID 141861.)

Some IDaaS providers extend their enterprise integration into unique areas. PasswordBank's Enterprise SSO offering, for example, includes the ability to manage time and employee attendance through integration with clock in/out systems (e.g., punch clocks) or through RFID, smart cards, or biometric devices. Mobile support is quickly becoming a must-have, and most of these vendors offer add-on products that provide cloud SSO to a wide variety of mobile devices and tablets.

Most IDaaS vendors provide support for strong authorization, either through their own interface or through integration with solutions from companies such as CrunchBase, RSA, SafeNet, Symantec, VASCO, and Yubico. This is another advantage of an IDaaS solution—because users can be channeled through a single portal, a software-based strong authentication solution can be located on the portal instead of installed on all the individual clients. For example, Intel's Expressway Cloud Access 360 offers an add-on feature (Nordic Edge One Time Password Server) that provides two-factor authentication for mobile clients by sending the one-time password to the device via SMS, email, chat, or mobile client app.

Getting access to SaaS applications isn't only about authenticating users. You must also efficiently manage the user accounts across hundreds or thousands of these applications. All the IDaaS vendors provide some kind of support for provisioning the user accounts into their service, but because SaaS providers generally charge for their service based on the number of users signed up for it, you don't want to create accounts in the service until they're needed. As a result, manual provisioning—preloading users from a worksheet or .csv file—isn't desirable. A better approach is directory synchronization, where users that are members of a particular AD security group (such as Salesforce Users) are automatically created in the cloud service and removed when a member leaves the group. Cloud account management is thereby done at the AD end of the equation. Just-in-time (JIT) provisioning takes this a step further. Even though the user might exist in the Salesforce Users security group in AD, a user account for a cloud service isn't created until the user attempts to access the service for the first time.

The connection between your enterprise and the IDaaS provider is clearly of great importance; without it, users will be unable to access their SaaS applications. If you use the most common configuration of utilizing a local agent to synchronize identities between your on-premises AD system and the IDaaS provider, the agent usually communicates via LDAP over SSL (LDAPS). If you configure the IDaaS connection to remain active only during the authentication of a user session, once users log on to an SaaS application, they'll communicate directly with the application and an IDaaS outage won't interrupt them. If you configure the connection to remain online for the entire session (for example, to get greater auditing detail), the connection must remain available at all times.

I'm instinctively a little uncomfortable with the snake-eating-its-own-tail feeling of basing one's access to cloud services on a cloud service. As failures have shown in the past, just being in a cloud service doesn't necessarily make it fault tolerant. So, you should look into the high availability architecture of any IDaaS service you're seriously interested in.

From Radical to Mainstream

Using IDaaS for identity management is quickly moving from a cutting-edge, radical idea that only small companies would try to a viable, mainstream identity-management option. IDaaS providers are now handling identity management for some very large enterprises. Although small or new companies might opt for an identity-entirely-in-the-cloud configuration, most companies will likely want to use an IDaaS solution as part of a hybrid on-premises/cloud solution. These companies will retain their existing investment in identity management but use a new identity model to accommodate the new cloud computing model.

InstantDoc ID 142290

Sean Deuby
(sean@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Pro*. He's been a directory services MVP since 2004.

Thursday, April 19, 2012

Leveraging VMware's Technology

eLearning Series
from Windows IT Pro

Join Alan Sugano, President of ADS Consulting Group, as he explores how you can leverage VMware's technology. Alan will present three technical sessions on three VMware topic areas that are relevant to any IT department currently running or considering migrating to a virtualized infrastructure using VMware and ESXi.

You'll learn how to avoid common pitfalls when implementing this technology. You'll get a down in the trenches view of how to implement this technology with tips for what works and what doesn't. Reduce your learning curve, get time-saving tips and tricks, and avoid roadblocks that can hamper your implementation effort.

http://elearning.left-brain.com/event/leveraging-vmware

Alan Sugano

Hosted Email Archiving

Providers that can archive your email in the cloud

by B. K. Winstead

It's easy to enumerate the reasons why archiving email to the cloud is a good choice for many organizations. Hosted email archiving solutions are easy to deploy, and you're offloading tedious management tasks (e.g., maintenance, monitoring) to the hosted email archiving provider. Plus, you can typically expect fixed monthly costs for the service. However, you have to be willing to accept that the provider has adequate security measures in place for your data and business needs, so choosing the right provider is a serious decision.

Paul Robichaux discusses how to choose between hosted email archiving and on-premises archiving in his article "Hosted Versus On-Premises Email Archiving" (January 2012, InstantDoc ID 140496). If you're not sure which method best suits your organization, I recommend checking out that article. This Buyer's Guide assumes you've settled on a hosted service as the best approach to meet your archiving needs. The accompanying table gives a glimpse at a few of the services available, but I highly recommend you do further research, as this is a quickly changing market segment.

Big Data and Its Implications

In the past, a consideration for hosted archiving services was the storage quota: how much data you could store with the service and how much it would cost if your storage needs increased. However, most hosted email archiving services now offer unlimited storage as a standard feature—that is, no mailbox quotas are imposed. In addition, most services let you import legacy data, such as old email messages from PSTs, when you start the service, although they might charge a fee for this feature.

All the providers that appear in this guide offer unlimited storage and let you bring legacy data. Simply put, what this means is that you can have hosted email archives that are huge. The question to ask yourself is whether that's a situation you want for your business. Your users, of course, will be thrilled if they can shuffle everything into the cloud, find it through a search when they want it, and never have to delete anything. Your legal department might think otherwise if they ever have to review that data for an e-discovery request.

While you're considering an email archiving solution, it's a good opportunity to also think about instituting a comprehensive email retention policy so that you're not archiving useless or unnecessary data. "What companies essentially do is a risk assessment," said Barry Murphy, cofounder and principal analyst for the eDJ Group. "They say, 'What's the risk that Joe Shmo is going to lose an email that would make him better at his job versus the risk that I would have to pay a lawyer $500 an hour to review that document should it ever come up in a case?' The popular wisdom is that most of what's in our email systems is junk, which is not necessarily a bad assumption."

An email archive can be an extremely valuable thing for both end users and your legal team. But if you let them become cluttered with useless messages, you'll find the value somewhat more questionable. Be proactive in your retention policies to maintain a useful archive.

Not All Email Is Equal

As you investigate your options for hosted email archiving services, you'll find that they offer features for life cycle management, which is important particularly if you have or are implementing some form of retention policy. Life cycle management lets you set how long you want a particular item to remain in the archive before it's deleted forever. Some services have a limited lifespan for items by default—make sure you know what the service you choose does so you won't be surprised when items start disappearing unexpectedly.

The popular wisdom is that most of what's in our email systems is junk, which is not necessarily a bad assumption.

You're also going to have cases where certain blocks of data might need different retention lengths in the archive than others. Legal holds are the obvious case here, but your business might have other reasons to make exceptions. As Murphy said, "Not all departments are created equal. Maybe the research and development group at a pharmaceutical company should keep their email longer because they have some really important stuff there, whereas a group of marketing assistants might not keep their email as long because the chance that they're creating deep intellectual property is a lot less than someone in R&D."

If you're in an organization with multiple departments with varying needs, having the ability to set different retention

lengths could be a useful feature—or indeed, necessary if you're frequently the target of litigation. And if you're archiving data that might be considered sensitive, whether the vendor encrypts your data in storage, as well as what method of encryption is used, could be deciding factors.

SLAs and Due Diligence

As with any hosted service, the standard caveats apply when choosing a hosted email archiving provider. Perform your due diligence, carefully assess the terms of the company's service level agreement (SLA), and ask your questions up front. Get familiar with the security certifications for data centers and know what your provider is certified for.

Company	Product	Price	Initial Setup Fee?	Supported On-Premises Exchange Server Versions	Works with Exchange Online/ Office 365?	Other Supported Email Platforms and/or Services	Is Anything Installed On Premises?	Archiving Methods	Encryption Methods	Administrative Interface
123Together.com 781-273-6245 800-967-3924 www.123together.com	123Together.com Hosted Email Archiving Solution	$4/user/month	No	2010/2007/2003/2000/5.5	Yes	All email platforms that support journaling	No	Exchange journaling	Advanced Encryption Standard (AES)-256	Web-based and GUI console
Mimecast 800-660-1194 www.mimecast.com	Mimecast Unified Email Management	$1–$6/user/month	$450–$1,000	2010/2007/2003/2000	Yes	Lotus Domino	Yes	Exchange journaling; email (SMTP) routing	AES-256	Web-based
Smarsh 866-762-7741 www.smarsh.com	Smarsh Electronic Message Archiving	Contact vendor	Yes, contact vendor	2010/2007/2003/2000/5.5	Yes	Most platforms, including Lotus Notes, GroupWise, and Sendmail	No	Exchange journaling	Transport Layer Security (TLS) in transit; AES-256 at rest	Web-based
Sonian 617-958-4000 www.sonian.com	Sonian Email Archiving	$4/mailbox/month; volume discounts available	No	2010/2007/2003/2000/5.5	Yes	Novell GroupWise, Google Apps, IBM Lotus Notes, Kerio Connect, Zimbra, and all other major email platforms	No	Exchange journaling; IMAP support for non-Exchange platforms	AES-256	Web-based
Symantec 800-721-3934 www.symantec.com	Enterprise Vault .cloud	Contact vendor	Yes, contact vendor	2010/2007/2003/2000	Yes	IBM Lotus Domino and Google Apps	No	Exchange journaling	AES	Web-based
USA.NET 800-653-0179 www.usa.net	USA.NET Email Archiving and Continuity Service	$2–$10/user/month	$250	2010/2007/2003/2000	Yes	Any platform capable of copying messages	No	Exchange journaling; copying messages at the inbound and outbound Message Transfer Agents (MTAs)	SSL	Web-based

Editor's Note: Some vendors you might expect to see in this Buyer's Guide said they didn't have a product that exactly matched the criteria or didn't respond to our requests for information about their products.

Ask for customer recommendations. As Paul Robichaux said in his article, "Run—don't walk—away from any vendor that makes it difficult for you to do [any] of these things."

In a lot of ways, the process of choosing a hosted vendor requires more work than picking software that you'd install in your environment. However, if you make the right choice, you should find that your email archiving needs will be well served in the cloud.

InstantDoc ID 142279

B. K. WINSTEAD
(bwinstead@windowsitpro.com) is a senior associate editor for *Windows IT Pro*, *SQL Server Pro*, and *SharePoint Pro*, specializing in messaging, mobility, and unified communications.

	Access/ Authentication	Is Retention Limited by Default?	Life Cycle Management?	Different Retention Durations for Different Items?	Examples of Available Reports	Other Features Included	Other Features That Can Be Added for Additional Charge
	LDAP integration	No	Yes	Yes	Activity by user; activity by UI action; activity by date; collection by mailbox; collection by date	Random sampling; role-based administration; dashboard data recovery; advanced search and discovery; tamper-proof email capture; export email per Securities and Exchange Commission (SEC) regulatory requirements; custom retention policies; full e-discovery functionality	Personal archive access
	Active Directory (AD) integration; OpenID Cloud/local passwords	No	Yes	Yes	Overview reports; inbound viruses and spam; email connections and rejections; communications reports	Email security and email continuity; integration for archiving and continuity in Research in Motion BlackBerry devices; email archiving in Apple iPhone and Windows Phone	Mobile access and continuity; mailbox management; stubbing; Outlook folder structure replication; email stationery management
	Managed by designated company administrators	No	Yes	Yes	Email message review; top 10 senders; total number of keyword violations per use		Smarsh Virtual Compliance Officer; smarshDLP data-leak prevention; smarshEncrypt email encryption; IM, text message, and social media archiving
	AD integration	No	Yes	Yes	Logons; UI activity; exports; new searches; search edits,; granted access	Role-based permissions to facilitate e-discovery; ability to export to .pst, .eml, .pdf, .html, .txt, and .nsf file formats	File archiving
	Security Assertion Markup Language (SAML) 2.0 integration with Active Directory Federation Services (ADFS)/HTTP Secure (HTTPS); username/password over HTTPS; Windows password complexity/usage policies can be enforced	No	Yes	Yes	Average number of messages per user; average message size per user; average search speed; number of user logons; number of searches performed/speed/search strings used per user; e-discovery reports on subject matter, number of custodians, email messages, legal holds, tags applied, reviewers in matter, etc.	Tamper-proof storage	IM archiving; social media archiving; always-on email continuity
	AD integration	Yes	Yes	Yes	Requested reports; summary reports; event reports; supervisor activity reports; review summary; assignments; forwards; retentions; hold reports	Business continuity; role-based access; message reviewing and tracking for Financial Industry Regulatory Authority (FINRA) and SEC compliance	

INSIGHTS FROM THE INDUSTRY

System Center 2012 RC Ships, Showcases Revamped Licensing and Branding Strategy

Over the past decade, Microsoft's System Center product family has historically arrived in two forms: confusing product nomenclature and branding, and a complex licensing model that could drive even the most seasoned Microsoft licensing pro into fits of head scratching and eye crossing. Realizing that creating befuddled customers wasn't a good product marketing strategy, Microsoft announced in January 2012—in addition to news that the System Center 2012 release candidate (RC) is available for download—that the company is drastically streamlining and simplifying its System Center licensing and branding efforts. Here are two of the biggest changes:

- Branding—All of the eight separate System Center product sub-brands, including Microsoft System Center Operations Manager and Microsoft System Center Virtual Machine Manager 2007, are now gone. Those products will become components of System Center 2012, the only product that remains as a separately branded entity. System Center 2012 will be offered in only two versions: a Standard edition and a Datacenter edition. The former is aimed at businesses with more modest virtualization and private cloud needs, whereas the latter is aimed at organizations with more aggressive ambitions for virtualization and the cloud.
- Licensing—I attended a press workshop about the private cloud on the Microsoft campus, and Microsoft's Garth Fort—general manager of the System Center and virtualization marketing team—was walking the group of assembled IT journalists through the legacy System Center licensing structure. Fort displayed a Byzantine licensing diagram that looked like something a minotaur could get hopelessly lost in, and suggested—with tongue partly planted in cheek—that Microsoft has provided a "rich" array of licensing options for the System Center family, which was met with chuckles and laughter from the press in attendance.

With the System Center Standard and System Center Datacenter licensing changes, Microsoft brings some sorely needed clarity to the System Center licensing picture. These licensing changes are also a shrewd business move on Microsoft's part that will undoubtedly prove painful for the VMware sales team. This is painful because System Center 2012 Datacenter edition licensing will cover an unlimited number of virtual machines (VMs) without incurring additional licensing fees, in contrast to VMware's more costly licensing options.

It's always interesting to see how Microsoft's goals and ambitions for its products change over time. However, System Center has been remarkably consistent with the company's original goals for the product, which was to help IT professionals more easily manage and administer their infrastructures. Back in 2009, I interviewed Brad Anderson, Microsoft's current corporate vice president of the Management and Security Division (MSD), about what Microsoft's priorities were at the 2009 Microsoft Management Summit (MMS). Here's a bit of what Anderson said back then:

> Customers want a single set of tools to command across physical and virtual assets. They don't want to have two. They're looking for a consistent way to manage their Windows environments, from the data center to their servers and across their data centers. And there's a whole lot of hype going on in the market about [the] cloud. And what we're communicating is that the conversations about the cloud are great conversations, and if you think about what Microsoft has been communicating with our Software Plus Services strategy, these conversations about private cloud versus public cloud, those fit right in line with what we've been communicating for years.

At the private cloud reviewer's workshop, Anderson stressed the knowledge that Microsoft has gained from managing its own public cloud infrastructure for massive cloud services such as Hotmail, Xbox Live, and Bing. With this knowledge, Anderson said that Microsoft hopes to push through into its private cloud offerings as well. "There are certain things you can only learn by doing," Anderson said. "We have a set of scar tissue and experiences that enable us to leverage those learnings to benefit our customers building private clouds."

Windows IT Pro has covered the System Center 2012 news from several angles. See "With System Center 2012, Microsoft Democratizes the Private Cloud" (January 2012, InstantDoc ID 141927) for Paul Thurrott's thoughts about what this news means for Microsoft's private cloud efforts. Also, see "Microsoft System Center 2012 Enables the Private Cloud" (January 2012, InstantDoc ID 141932) to learn more about changes made to VM management.

—Jeff James

InstantDoc ID 141929

Finding Confidential User Information with Exchange Search

The nature of people who attend advanced training sessions is that they often pose some pretty thought-provoking questions. Paul Robichaux and I recently participated in the "Becoming an Exchange 2010 Maestro" event in which we had some intense discussions about various aspects of Microsoft Exchange Server deployment. During the question-and-answer session at the end of the event, I was asked, "Can I use Exchange 2010's search capabilities to find passwords that people have stored in their mailboxes?"

The answer is absolutely! Exchange Server 2010 doesn't apply restrictions to searches that administrators execute. This is because Exchange assumes that administrators know what they're doing when they execute searches against user mailboxes. More importantly, administrators have been granted this ability by their company in full knowledge that confidential information will most likely be revealed during a search. After all, isn't this the reason administrators perform searches?

Exchange protects users against casual searching. This type of search is performed by officials who have access to confidential information that's held by governments and public authorities. Exchange protects users by requiring administrators to be members of the Discovery Management role management group before they can create and execute mailbox searches. Furthermore, search results can be directed to a Discovery Search Mailbox that's only accessible to specific individuals that might not include administrators. This arrangement creates a division of responsibilities between users who execute the searches and users who review the search results.

If you want, administrator auditing can be enabled to capture information about new searches and mailbox audits in the Discovery Search Mailbox to track actions performed against the items in a particular mailbox. Auditing isn't perfect because it won't tell you if someone browses the items that are copied into the Discovery Search Mailbox by a search. At the end of the day, you'll need to adhere to the age-old principle that the ability to execute an action should only be assigned to users who have good reason to perform that action. In addition, these privileges should be reviewed frequently to ensure that user data can't be compromised.

Getting back to the original question, it's entirely possible that a rogue administrator might create a search that scans all user mailboxes to look for email that contains passwords and login information that users have stored. Given that so many websites send login details such as new password information and password reminders to users through email, it's not surprising that this data lingers in mailboxes. Sites run by banks and other financial institutions don't typically send sensitive data through email, but that doesn't mean that users don't use Exchange as a convenient storage repository to hold information that might be needed in the future. After all, powerful search functionalities that are offered by email clients make it easy to find login information in the blink of an eye.

How would a rogue administrator rummage through user mailboxes to look for password data? Roughly the same steps that are required for both on-premises Exchange 2010 and Exchange Online in Office 365. Here are steps that you can take to create and execute a multi-mailbox search to find confidential user data.

First, make sure that you're a member of the Discovery Management role group. An administrator can add himself to the Discovery Management role group by running the *New-ManagementRoleAssignment* cmdlet or by using the Exchange Control Panel (ECP).

Next, make sure that you have access to the Discovery Search Mailbox that will be used to store copies of items that match the search criteria. By default, members of the Discovery Management role group have full access to the default search mailbox that's created when the first Exchange 2010 mailbox server is installed in an organization. If you create additional Discovery Search Mailboxes, you'll have to assign access to those mailboxes before they can be opened. For on-premises Exchange 2010, you can use the Exchange Management Console (EMC) to grant full access to the mailbox. For Office 365, you need to follow the steps described in the Microsoft article "Give Users Access to Multi-Mailbox Search" at http://help.outlook.com/140/ee424426.aspx.

Once you have the necessary privileges, you can go to the ECP and select *Manage My Organization* and go to the Reporting node or Mail Control for on-premises Exchange 2010 and Office 365, respectively. You can then create a new multi-mailbox search and specify search criteria. For example, you might search specific mailboxes or scan all the mailboxes in the organization up to a limit of 25,000 mailboxes by default in one search. See the Microsoft article "Exchange 2010 Discovery: Modify the maximum number of mailboxes searched at a time" at http://tinyurl.com/3hk4b6p to increase the maximum number of mailboxes for a single search.

When you're ready, you can start the search and wait for it to complete. Exchange will send you a message when the results are ready. Depending on the number of mailboxes that are searched and the number of items in each mailbox, a search might take anywhere from a few minutes to a few hours to complete. Eventually the search will complete and you'll be able to open the Discovery Search Mailbox to find out what's been discovered.

For all situations regarding management of systems that contain confidential user data, the only way to protect against administrator abuse is to set clear expectations of when discovery searches are appropriate, who can authorize these operations, what happens to the data that's found, who can access that data, and the consequences that follow if someone oversteps the mark. You wouldn't let an administrator delete a user mailbox without some form of control, and the same degree of oversight is required for discovery searches. In fact, this is a great example of how features should be reviewed as new versions of software are deployed to ensure that administrator responsibilities are kept updated.

—Tony Redmond

InstantDoc ID 141627

Why Object Storage Will Take Over the Cloud in 2012

In 2011, object storage started to gain major traction in the market, especially because it had been validated by companies such as Amazon, Google, and Facebook, which use this type of architecture to power their very large infrastructures and petabyte-sized implementations. Mark Goros, CEO of Caringo, shared five reasons why he believes object storage will take over the cloud infrastructure in 2012:

1. Object storage will bring cloud economics to any organization in 2012—A key to the affordability delivered with cloud storage is to begin with commodity components in a redundant, multi-tenant architecture with highly efficient disk utilization. These benefits are driven by object storage infrastructure, which most assume is due to economies of scale and proprietary development. However, advancements in object storage, including significant progress in standardization of interfaces and a maturing ISV ecosystem, are making object storage one of the best options for organizations looking to cost-effectively store their unstructured data.

2. The relentless growth of data will expose the limitations of SAN and NAS—The complexities and costs of traditional NAS and SAN storage arrays will continue to become increasingly prohibitive as a viable long-term storage option for unstructured data. Information created by organizations will need to be stored and accessible for indefinite periods of time, driven by the ability to re-use and by regulatory compliance purposes. Object storage will be one of the few ways that organizations can easily and cost-effectively store massive libraries of information that are instantly accessible.

3. Object storage will enable the adoption of hybrid and private cloud solutions—Organizations will increase their adoption of hybrid and private cloud storage solutions as IT departments look to solve management and cost issues associated with data growth. The move to hybrid and private cloud solutions will be based primarily on the ability to guarantee the security and integrity of their information while still benefiting from cloud economics.

4. Object storage will help with file count in addition to storage capacity—In addition to an increase in capacity, organizations are also seeing an increase in the number of files driven by "Big Data" applications, research equipment, and continued optimization of web-delivered information. These files range from a few kilobytes to tens of terabytes and are exposing the limitations of file systems. As the number of files increases, file systems become less responsive, requiring IT to purchase new storage systems to increase performance and responsiveness instead of capacity. Organizations will turn to object storage to provide a flat and highly efficient address space with no limit in file count or capacity.

5. Data growth will prohibit backups—As data sets grow, backup windows get longer and longer until they ultimately become unmanageable and IT must decide what data to back up or, even worse, not back up at all. Object storage will be turned to as organizations realize that they can use file replication and integrated self-healing, self-optimization, and metadata-driven data lifecycle management to eliminate backups altogether.

—Jason Bovberg

InstantDoc ID 141901

3 Bits of Advice Regarding the Cloud

"If you're a company that was 50 users and is now 200 users, supporting them is enormous, especially with mobile devices. Servers in a data center, that's one thing—now you're supporting mobile endpoints," says Jeff Kaplan, CEO and founder of Breakthrough Technology Group (BTG), an AT&T Channel Solutions partner, and provider of private cloud builds, hosted services, telecomm services, and mobile app development.

"With such a proliferation of devices, people want a common experience. The piece that is coming is the desktop in the cloud [VDI]," Kaplan says. Customers are looking for uniformity, he says.

"The big cost model is the desktop—every three to four years you have to move to a new version, you have to protect, run backups, run a Help desk. We're taking the entire computing environment and making it available."

Kaplan offers 3 tips for organizations considering moving to the cloud:

1. Don't take a siloed approach—It helps to go with a managed service provider that allows for scalability. With BPOS, Kaplan says, "You didn't have VDI; you had to have a different Help desk for Microsoft solutions, you had to have different processes." Don't take a siloed approach, he says, but rather "Think integrated."

2. IT needs to decide what's needed—Managed service providers offer management in various ways, from infrastructure to apps. It's up to IT to decide what they're looking for, whether it's help with patching and management, or more.

3. Focus on the right business strategy for scaling—"Make sure that you don't do something to back yourself in a corner," Kaplan says. "Every app is now mission-critical. It needs to be up 24 × 7 and perform well. You have to build the correct architecture, and you need business continuity."

According to Kaplan, "Bandwidth is key; we understand that. Carriers are pushing 4G. Hardware vendors are buying up cloud-based storage. They're getting themselves ready. Everyone's getting ready for a time when everything is a central computing model and you get there with ease. When you talk about convergence, it's a convergence of industries and product sets. And we combine that."

—Caroline Marwitz

InstantDoc ID 141026

AD INDEX

For detailed information about products in this issue of *Windows IT Pro*, visit the websites listed below.

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/go/forums

News

Check out the current news and information about Microsoft Windows technologies.
www.windowsitpro.com/go/news

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

DevProConnections UPDATE
Exchange & Outlook UPDATE
Security UPDATE
SharePoint Pro UPDATE
SQL Server Pro UPDATE
Windows IT Pro UPDATE
WinInfo Daily UPDATE

www.windowsitpro.com/email

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles:
penton@wrightsmedia.com

Windows IT Pro VIP

Get exclusive access to over 40,000 articles and solutions on CD and via the web. Includes FREE access to eBooks and archived eLearning events, plus a subscription to either *Windows IT Pro* or *SQL Server Pro*.
www.windowsitpro.com/go/vipsub

SQL SERVER PRO

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

ASSOCIATED WEBSITES

DevProConnections

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
www.devproconnections.com

SharePoint Pro

Dive into Microsoft SharePoint content offered in specialized articles, member forums, expert tips, and web seminars mentored by a community of peers and professionals.
www.sharepointpromag.com

NEW WAYS TO REACH *WINDOWS IT PRO* EDITORS:

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at: http://tinyurl.com/d5bquf. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

Windows IT Pro

Ctrl+Alt+Del

by Jason Bovberg

"Send your funny screenshots, oddball product news, and hilarious end-user stories to rumors@windowsitpro.com. If we use your submission, you'll receive a *Windows IT Pro* Rubik's Cube."

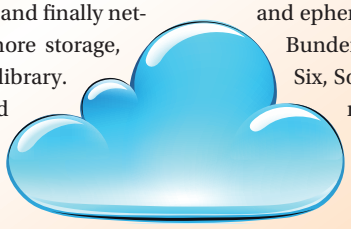
Cloud Computing Revealed as Hoax

Amazon Kindle marketing associate says she made it up over lunch

Seattle, Washington — Shawna Bogan, Amazon junior marketing associate on the Kindle team, revealed on Tuesday that she invented cloud computing on a lunch break in April 2008. The revelation sent shockwaves through an industry that has been gradually building a foundation on such market-speak as "hosted services," "Software as a Service," "cloudsourcing," and "cloudstorming," among other ridiculous nonsense. Indeed, the market has seen an explosion of new business ventures whose very existence hinges on a notion that is now revealed to be false.

"We were all just sitting around in the break room," Bogan said, "trying to figure out how to explain that all of Amazon's Kindle titles were stored on a PC under my desk. I suddenly realized that, since no one would actually see my PC, the files could be anywhere—even up in the sky."

As the Kindle library of books began to grow, so did the storage capacity of Bogan's PC. With the help of an Amazon Help desk temp, she quietly added storage space, and finally networked an old Compaq system for even more storage, with which to contain the expanding Kindle library.



"People must think all this stuff is stored securely on massive servers somewhere," Bogan said, peeking under her desk with a laugh. "I think it's time people knew the truth. I'm sure this is the same way all these new companies are doing it, too." She paused, considering. "I should probably put some antivirus on there."

Following Bogan's revelation, other prominent cloud companies admitted to buying into the hoax and propagating it with their own offerings. "We knew we could never afford to compete if we took the time and expense to actually construct real, massive data centers," said Beezil Shoshugani of RackSaaS. "And why bother when we could do it all with in-house hard drives? But we thought we were the only ones doing it that way. I'm not sure how I feel to learn that we hadn't really found a loophole after all."

When informed of this news, Microsoft's Steve Ballmer said, "I knew it! I knew it! The whole idea was stupid from the start!" Ballmer has been famously reported to say that Microsoft is "all in" on cloud computing. "First they get me dancing around in YouTube videos like a giant sweating monkey, and now this," Ballmer said. In related news, Ballmer's personal speech writer and PR team are rumored to have been fired.

Industry analyst Niles "Nimbo" Stratus, vice president of Superior Thin Research, predicted the revelation would have little to no effect on the market. "Every industry vertical we touch is resourced around enhancing the benefits of a robust and pliable revenue stream, ephemeral or otherwise. Whether ECM, ARP, PNZ, or ORC, they understand the need to subsume and strategize their productivity, as users continue to optimize and reify the trivially enable-able low-hanging fruit collaboratively, in real time. And really, the mandate is there to monetize and maximize the resulting output. Especially when v2 releases."

News that cloud computing has been proven to be fluffy and ephemeral didn't surprise some IT professionals. Clem Bundershoot, a Windows support technician from Ninety Six, South Carolina, wasn't shocked by the news. "I told my boss that all that talk about the cloud was just nonsense," Bundershoot said. "Cloud this, virtualization that, and all that other crap about people using those Apple toy computers and phones. I knew the liberal media was puffing it all up. Everyone knows that real IT is done with real hardware that you can see and touch. You can take your virtual this and cloud that and stick it where the sun don't shine."

Meanwhile, asked if she expected fallout from revealing the truth about cloud computing, Amazon's Bogan said, "Not really. I was surprised it went this far, to be honest, and I just felt it was time for the story to be told. I would get in real trouble if I ever told you what Amazon is doing with people's credit card numbers and other personal information. It's shocking. But I would never do that, of course."

—Contributing reporters: Sean Deuby, Jeff James, Caroline Marwitz, and B. K. Winstead

April 2012 issue no. 212, *Windows IT Pro* (ISSN 1552-3136) is published monthly. *Windows IT Pro,* 748 Whalers Way, Fort Collins, CO 80525, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 748 Whalers Way, Fort Collins, CO 80525. Advertising rates furnished upon request. Periodicals Class postage paid at Fort Collins, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,* 748 Whalers Way, Fort Collins, CO 80525.** SUBSCRIBERS: Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, 748 Whalers Way, Fort Collins, CO 80525. Printed in the USA.

NEW!

CLOUD SERVER CONTROL AT YOUR FINGERTIPS

Only pay for what you need.
Change your server specifications anytime!

- Adaptable with up to 6 CPU, 24 GB of RAM, and 800 GB hard drive space
- On-the-fly resource allocation – hourly billing
- Dedicated resources with full root access
- Linux or Windows® operating systems available with Parallels® Plesk Panel 10.4
- Free SSL Certificate included
- 2,000 GB Traffic
- 24/7 Hotline and Support
- 1&1 servers are housed in high-tech data centers owned and operated by 1&1

1&1 DYNAMIC CLOUD SERVER

3 MONTHS FREE!*

Base Configuration, then $49/month

NEW: Monitor and manage servers through 1&1 mobile apps for Android™ and iPhone®.

MEMBER OF united internet

1-877-461-2631 www.1and1.com

1-855-221-2631 www.1and1.ca

1&1®

* 3 months free based on the basic configuration ($49/month) for a total savings of $147. Setup fee and other terms and conditions may apply. Visit www.1and1.com for full promotional offer details. Program and pricing specifi cations and availability subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet, all other trademarks are the property of their respective owners.

Microsoft

Meet, share, and edit documents from 6,000 miles away.

It all works together.

Now you can collaborate in the cloud and edit documents from virtually anywhere with a comprehensive suite of integrated tools: Office, Exchange, SharePoint, and Lync videoconferencing. **Starting as low as $8 per user per month. Begin your free trial now at Microsoft.com/office365**

Scan tag with a smartphone to learn about the Office 365 free trial.
Download the free scanner app at http://gettag.mobi

Microsoft® Office 365